NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPLEMENTATION OF PHASED ARRAY ANTENNA TECHNOLOGY PROVIDING A WIRELESS LOCAL AREA NETWORK TO ENHANCE PORT SECURITY AND MARITIME INTERDICTION OPERATIONS

by

Andrew P. Rivas

September 2009

Thesis Advisor: James Ehlert
Co-Advisor: Albert Barreto

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Implementation of Phased Array Antenna Technology Providing a Wireless Local Area Network to Enhance Port Security and Maritime Interdiction Operations		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Andrew P. Rivas			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	
13. ABSTRACT (maximum 200 words) This thesis will focus on field testing to evaluate the feasibility of employing electronically steered (phased array) antennas to provide a ship-to-shore wireless network connection (802.11g) for littoral maritime assets. Specific areas being examined included the evaluation of voice, video, and other data transmitted from a maritime interdiction team, in real time, to a remote command and control center in support of a Visit Board Search and Seizure (VBSS) and Maritime Interdiction Operations (MIO).			
14. SUBJECT TERMS MIO, VBSS, electronically steered antenna, phased array antenna, wireless network connection, Wi-Fi, IEEE 802.11g, boarding team, COTS, WLAN, smart antenna, OpenVPN application, wireless base station, OFDM, latency, point-to-point wireless link.			**15. NUMBER OF PAGES** 101
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

IMPLEMENTATION OF PHASED ARRAY ANTENNA TECHNOLOGY PROVIDING A WIRELESS LOCAL AREA NETWORK TO ENHANCE PORT SECURITY AND MARITIME INTERDICTION OPERATIONS

Andrew P. Rivas
Lieutenant, United States Navy
B.S., Texas A&M University, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2009

Author: Andrew P. Rivas

Approved by: James Ehlert
Thesis Advisor

Albert Barreto
Co-Advisor

Dr. Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis will focus on field testing to evaluate the feasibility of employing electronically steered (phased array) antennas to provide a ship-to-shore wireless network connection (802.11g) for littoral maritime assets. Specific areas being examined include the evaluation of voice, video, and other data transmitted from a maritime interdiction team, in real time, to a remote command and control center in support of a Visit Board Search and Seizure (VBSS) and Maritime Interdiction Operations (MIO).

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
BOQ	Bachelor Officer Quarters
C^2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CNO	Chief of Naval Operations
CO	Commanding Officer
COASTS	Cooperative Operations and Applied Science & Technology Studies
COC	Chain of Command
CONOPS	Concept of Operations
COTS	Commercial off the Shelf
dB	Decibel
DoD	Department of Defense
DSSS	Direct Sequence Spread Spectrum
ERP	Extended-Rate Physical (ERP-OFDM)
FCC	Federal Communications Commission
FEX	Field Experiment
FHSS	Frequency Hopping Spread Spectrum
GPS	Global Positioning System
GWOT	Global War on Terror
HR/DSSS	High Rate/DSSS (see DSSS above)
IEEE	Institute of Electronic and Electrical Engineers
IP	Internet Protocol
ISM	Industrial Scientific Medical
ISP	Internet Service Provider
ISR	Intelligence, Surveillance, and Reconnaissance
JOCC	Joint Operations Command Center
Kbps	Kilobits per second
kHz	Kilohertz

LAN	Local Area Network
LOS	Line of Sight
Mbps	Megabits per second
MHz	Megahertz
MIO	Maritime Interdiction Operations
NM	Nautical Miles
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PCF	Fast Patrol Craft
PTMP	Point-to-multipoint
PTP	Point-to-point
RF	Radio Frequency
RTN	Royal Thai Navy
SBU	Sensitive but Unclassified
SSL/TLS	Secure Socket Layer/Transport Layer Security
TAO	Tactical Action Officer
UPS	Uninterruptable Power Supply
USCG	United States Coast Guard
USN	United States Navy
UTB	Utility Boat
VAC	Voltage Alternating Current
VBSS	Visit Board Search and Seizure
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

ACKNOWLEDGMENTS

I would like to begin by thanking my best friend and beautiful wife Dee Anne because *“behind every successful man, there is a woman who puts up with a whole ‘lotta crap.”*——Origin Unknown

Dee Anne, thank you for putting up with me, and the kids, ever since we have been in the Navy, but especially throughout the past year. Without your love and support, and frankly your never-ending patience, this thesis would not have been possible.

Pat——truly my thesis testing brother-in-arms, probably more like partner in crime, and an irreplaceable friend—you are a one-stop shop for motivation and technical knowledge. Thanks for hanging in there with me through this entire ordeal we have defined as “testing and documentation.” I guess you won’t need my water bottles any more, seeing as how you quit dipping——good on you!

Jim, thanks for guiding me to this thesis topic and for pointing me in the direction of Ryan and John and then turning me loose.

Ryan “Twister” Hale——the man behind the laptop, behind the curtain——thanks for all of your hard work and dedication. We (the Tripod) know how hard you worked behind the scenes——you always made time to teach us and answer our questions. We truly appreciate your support and sacrifice to help us get our theses done.

John “MacDaddy” Spracklen——your friendship, willingness to teach and advise us, and overall direction made this

research possible. Thanks for all of the help, on-site and long distance, including setting up and troubleshooting the panels over the phone. You bring new meaning to the term “taking one for the team.” John, thank you for everything, and I hope that you and your family live a happy and blessed life——you guys deserve it. Good luck and God Bless John.

There are too many people to formally recognize and individually thank for assisting me in the thesis writing process. To all of you who are not mentioned—*especially* Buddy and Jane Barreto——I truly thank you for your help with completing this research.

I. INTRODUCTION

A. BACKGROUND

The threat of terrorist attacks against the United States and its interests worldwide has prompted development of our current national maritime strategy, which emphasizes the security of ports and the global maritime commons.[1] This daunting task of providing global stability to promote worldwide economic commerce has specific tenants that will rely primarily on the exchange of information over networks.

The ultimate objective is to deliver timely intelligence, surveillance, and reconnaissance (ISR) necessary to achieve situational awareness by tactical and strategic decision makers throughout the chain of command and laterally among multinational partners and regional military and law enforcement through information sharing. Critical aspects of this objective are providing seamless wireless network coverage for littoral assets and the security of the sensitive but unclassified (SBU) information exchanged between multinational and DoD assets.

Any wireless network infrastructure is only as good as its ability to provide security for users and information. The rapid advancements in network components, secure wireless communications, and mobile data devices have made possible the practical use of wireless networks in many current military and law enforcement applications in a variety of environments.

[1] Chief of Naval Operations, "Cooperative Strategy for 21st Century Seapower." October 17, 2007.

B. VISION

Imagine the possibilities of a remote command and control (C^2) cell in Manama, Bahrain, capable of watching a live video feed from a boarding, in support of Maritime Interdiction Operations (MIO), taking place in the vicinity of the Al Basrah Oil Terminals. Consider the benefits of key decision makers and intelligence analysts having instant access to real-time updates and raw intelligence gathered from the boarded vessel and its personnel by the Visit, Board, Search, and Seizure (VBSS) team members. Moreover, envision the value-added capability of the boarding team members capturing biometric data from the vessel's crew and transmitting it from a laptop, deployed with the team onboard the vessel, to a biometric database located in Virginia for documentation and comparison against known or suspected terrorists. Think of the potential force multiplier of the boarding team's ability to instantly transmit images of contraband, significant documents or intelligence, and observations made during the conduct of the boarding, in real time, without ever leaving the vessel's pilothouse. The time and cost savings in manpower and tasking, and the reduction of risk in an unpredictable operating environment presents an intriguing prospect to leverage current and emerging wireless network technologies.

C. APPLICATION

Maritime security operations including port security, law enforcement, and MIO continue to be increasingly important missions in the Global War on Terror. Inherent to these constantly evolving mission areas is the ability of

the operator (VBSS boarding team member) to gather and quickly disseminate vital information in the form of documents, images, biometric data, and intelligence information for documentation and increased situational awareness. Sensitive information must get into the hands of the appropriate users, intelligence analysts and tactical decision makers, as quickly as possible. Current procedures for data, information, and intelligence gathering during a MIO boarding does not allow for digital transmission to the end users until after the VBSS team has completed the evolution or has physically returned portions of the information or data to its base of operation or afloat unit. The current process of transmitting information can take hours, depending on the size of the boarded vessel, its crew, and the amount if intelligence or information gathered. The current methodology is extremely inefficient and results in time-late information to the end users, and places an enormous stress on the unit’s watchstanders supporting the boarding process. MIO boardings frequently place a heavy burden on voice communications between the boarding officer, on the vessel being boarded, and the afloat naval unit, creating unnecessary distractions for the VBSS Team as the chain of command constantly prods for progress updates throughout the conduct of the boarding and clarification of information passed over the tactical voice networks.

Research will focus on the evaluation of the applicability and feasibility of employing shore-mounted electronically steered (phased array) antennas to provide a ship-to-shore wireless network connection for assets operating in the littoral maritime environment. Field

testing areas being examined include the evaluation of video, voice, and data transmission via a laptop to a remote command and control center from a VBSS Team member conducting a MIO boarding on a vessel which is either or anchored. Utilizing the described wireless network technique, the boarding team could broadcast all information, video, biometric data, and so forth to the entire MIO chain of command simultaneously, enabling MIO boardings to become safer for the VBSS teams, quicker in execution, and provide higher utility in the area of intelligence gathering and documentation.

From a C^2 perspective, the MIO commander, ship Commanding Officer (CO), and all respective tactical action officers (TAOs) and watch captains would all have real-time situational awareness (SA) and updates as to the conduct and progress of the boarding. Intelligence specialists would be able to receive key items of interest as they are discovered onboard the vessel of interest, instead of hours after the vessel has been released and the boarding secured.

II. TECHNOLOGY BACKGROUND

A. 802.11G WIRELESS PROTOCOL

1. Wireless Technology Advantages

The use of wireless technologies, 802.11b/g Wi-Fi specifically, has many key advantages for the end user given specific operational situations. Wi-Fi is analogous to the IEEE 802.11 standard that operates in the 2.4GHz frequency spectrum. It is the most widely implemented wireless LAN (WLAN) technology defined by the Institute of Electrical and Electronics Engineers (IEEE) and regulated by the Federal Communications Commission (FCC) in the United States. The FCC has designated the 2.4–2.5GHz, Industrial Scientific Medical (ISM), frequency band as a license-free band for radio communications. This means that to operate in this frequency spectrum, one is not required to acquire any license or pay any fees as long as the equipment is authorized by the FCC. Operating in accordance with the FCC regulations also means that any WLAN equipment utilizing this ISM band for radio communications must adhere to the designated radio frequency, output levels, and indoor/outdoor environment requirements and limitations. The specifics of the equipment settings and limitations will be discussed later in this section.

Given the regulations of the FCC, it is relatively easy to employ Wi-Fi WLANs as most of the technology, regardless of vendor or manufacturer, can be integrated in a plug-and-play fashion. The Wi-Fi Alliance has gone to great lengths

to ensure that Wi-Fi Certified products are standardized and interoperable as to further the use of the 802.11b/g wireless spectrum regardless of the manufacturer. This COTS interoperability mentality allows for ease of use and flexibility with networking component choices.

Wi-Fi has a small physical footprint when compared to other wireless spectrum equipment. The deployment of antennas and their location can be less precise, as they do not need not be aligned and or sighted in to operate. The 2.4GHz signal emitted from wireless antennas covers the specific range of the transmitter. As long as the receiver (antenna) is within LOS of the maximum effective range of the transmitting wireless antenna or access point, a link can be made and sustained. This can be accomplished with very little equipment on the receiving end, as this relates to the specific application of the technology outlined below.

Mobility and flexibility are huge advantages associated with Wi-Fi wireless technology. The option to wirelessly transmit information while in a remote location back to a wired network center or operations is a huge advantage that can be exploited. During a MIO Boarding, an emphasis is placed on voice communications to coordinate efforts between remote operators and the chain of command on a ship or at a specific C^2 operations center. Wireless technology and the ability to communicate utilizing multiple means is an important aspect of C^2 as well as SA. A wireless link between the CoC and physically remote operators can also

serve as a redundant form of communications if voice communications fail or cannot be used due to the operational environment.[2]

2. OFDM

Orthogonal frequency division multiplexing (OFDM) is a digital modulation mode that divides a wireless signal into multiple sub-carriers of different frequencies, across a designated frequency band, and transmits them in parallel.

a. Orthogonality

Orthogonality, as it applies to general use and/or information technology vice complex mathematics, means to have the characteristic of independence and the ability to be utilized without it impacting something else.[3]

b. Frequency Division and Multiplexing

The 802.11g carrier signal is divided into several subcarriers, each for the transmission of data, each at different frequencies across the frequency band. These multiple narrowband signals are then multiplexed into a single combined channel and transmitted simultaneously across the wireless medium.[4]

---

[2] Tom Carpenter and Joel Barrett, Certified Wireless Network Administrator (CWNA) Official Study Guide, Fourth Edition. August 17, 2008, 5-18.

[3] Matthew Gast, 802.11 Wireless Networks: The Definitive Guide, Second Edition. April 25, 2005, 276–310.

[4] Ibid.

c. 802.11g Variant

OFDM is generally associated with 802.11a technology, the IEEE 802.11 amendment in which it was first introduced, however, the 802.11g variation is known as extended-rate physical OFDM (ERP-OFDM). This specifically differentiates the changes made to the technology implemented in the 2.4GHz ISM band (802.11g) from the original OFDM technique used in the 5GHz frequency band (802.11a).

d. ERP-OFDM Advantages

By employing this method of spreading the signal across the spectrum——theoretically not "spread spectrum technology," but closely related——OFDM facilitates the use of a range of frequencies to transmit information at lower power levels. This, in turn, makes the wireless signal(s) extremely resistant to interference because of the lower power levels used in transmission. Because the (subcarrier) signals are transmitted over slightly different frequencies, multiple redundant communication signals are created which ensure that the signal is received, if the operating environment prevents the transmission of one of the frequencies. Another benefit of this transmission technique is that it prevents the overlap of bits (data) from reflected signals at the receiver, known as multipath distortion or intersymbol interference. The two most evident advantages of ERP-OFDM are greater spectral efficiency and the capacity for higher data rates.[5]

[5] Carpenter and Barrett, Certified Wireless Network, 117-125.

3. Data Rate vs. Throughput

An important distinction should be made between throughput and data rate, and to some extent bandwidth, and how these terms relate to wireless network technology. Bandwidth can be compared to the diameter of a pipe, as the pipe represents the path of wireless communications. In this analogy, the diameter of the pipe represents the wireless spectrum available for the transmission of data, just as it physically represents the capacity to deliver fluid through it. Bandwidth is merely an indicator of the physical capacity to transmit data at designated rates. For this reason, the units associated with bandwidth should be megahertz (MHz) or kilohertz (kHz), which are measurements of the range of a given frequency band. Bandwidth should not be associated with the rate of data transmission, commonly measured in megabits per second (Mbps) or kilobits per second (Kbps).

Throughput is the amount of functional data that is intentionally transferred across the wireless medium, or through the pipe. The data rate, or the rate at which this is accomplished, is a measure of the intended and the unintended data, such as overhead. As alluded to in the sections above, much of the designated frequency spectrum available for data transfer across the wireless medium is occupied by management frames, network protocols, and redundant data transmissions encoded into the wireless signals, all of which is collectively referred to as overhead. Because of overhead, the throughput of wireless networks will always be less than the advertised data rate.[6]

[6] Gast, 802.11 Wireless Networks: The Definitive Guide, 529.

Think of the data rate as a rating, just as piping systems are rated up to a maximum pressure setting. The operational pressures experienced by piping systems are normally much less than the maximum rating. The same is true for the actual throughput experienced in wireless communications. As illustrated in Table 1, rarely is the maximum value (data rate) reached in day-to-day wireless network operations. It is for this reason that the throughput is measured to represent the amount of actual data intended for transfer over the wireless network.[7]

PHY	Standards Introducing the PHY	Data Rate	Estimate of Throughput
FHSS	IEEE 802.11-1997	1–2 Mbps	0.7–1 Mbps
DSSS	IEEE 802.11-1997	1–2 Mbps	0.7–1 Mbps
HR/DSSS	IEEE 802.11b-1999	1, 2, 5.5, and 11 Mbps	3–6 Mbps
ERP	IEEE 802.11g-2003	1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbps	3–29 Mbps
OFDM	IEEE 802.11a-1999	6, 9, 12, 18, 24, 36, 48, 54 Mbps	3–29 Mbps
HT	IEEE 802.11n-2009	1–600 Mbps (with 4 spatial streams)	Untested

Table 1. Estimated throughput of data rates of wireless technology standards (from CWNA Official Study Guide, 4th ed.).

The easiest way to maximize the throughput on an ERP-OFDM wireless antenna system is to configure the hardware or antenna set to transmit in “g only mode.” The fact that the

[7] Carpenter and Barrett, Certified Wireless Network, 117-125.

antenna must send out redundant signals and then convert them to 802.11b, from 802.11g, reduces the throughput of the antenna. This reduction in throughput is a direct result of increased overhead needed to make these conversions at the antenna.

B. PHASED ARRAY ANTENNA TECHNOLOGY

Phased array antennas are actually a system of multiple antennas that are connected to a signal processor. Adjustments are made to each of the antennas' signal strength and phase of signal transmission to form narrow, directed RF beams of energy. These individual beams of RF energy can be directed, or electronically steered, in different directions without the antenna ever moving. Instead of rotating the antenna to change the direction of the RF energy to cover a given area, the antenna remains stationary and the RF energy beams are directed to the client(s) as needed. This type of antenna technology is utilized in many air defense radar applications.

1. Smart Antenna System

A smart antenna must be able to electronically direct the RF energy beams directly to the wireless client, or receiving antenna. A technique utilized to accomplish this task over the coverage area of the base station is called beam switching. The base station will scan pre-determined coverage beams and as wireless clients are identified and authenticated the transmission of information across the wireless link occurs.[8]

[8] Carpenter and Barrett, Certified Wireless Network.

2. FCC Rules for Antenna Output Power

In the United States, the FCC regulates the maximum output power of antennas based on their environment, frequency band, and type of link made, and the type of antenna. For the purposes of this thesis, we will concentrate on phased array antennas utilizing the 2.4GHz ISM band outdoors.

a. PTP/PTMP Links in 2.4GHz ISM Band

There are two distinct categories of wireless links regulated by the FCC: point-to-point (PTP) and point-to-mulitpoint links (PTMP). For PTMP links, the output power of the antenna must not exceed 4 watts. In addition, the total output power at the point of radiation, known as the intentional radiator, must be reduced by 3 decibels (dB) for every 3 dB of passive gain at the antenna. Passive gain is achieved by focusing or directing the output power of the signal in a desired direction. PTP links must not exceed 1 watt of output power at the intentional radiator. Also, the output power must be reduced by 1 dB for every 3 dB of antenna gain *above* 6 dBi. The limits of the PTMP and PTP links are illustrated in Tables 2 and 3, respectively.

Intentional Radiator Power (dBm)	Antenna Gain (dBi)	EIRP (dBm)	EIRP (watts)
30	6	36	4
27	9	36	4
24	12	36	4
21	15	36	4
18	18	36	4
15	21	36	4
12	24	36	4

Table 2. PTMP power limit table for 2.4GHz ISM band (from CWNA Official Study Guide, 4th ed.).

Intentional Radiator Power (dBm)	Antenna Gain (dBi)	EIRP (dBm)	EIRP (watts)
30	6	36	4
29	9	38	6.4
28	12	40	10
27	15	42	16
26	18	44	25
25	21	46	39.8
24	24	48	63
23	27	50	100
22	30	52	158

Table 3. PTP power limit table for 2.4GHz ISM band (from CWNA Official Study Guide, 4th ed.).

Most engineers would agree that a phased array antenna system would fall under the rules as defined by the FCC for PTMP links. However, because phased array antennas

are able to direct narrow beams of RF energy directly to clients, these systems operate under an exception to the PTP link power limits.[9]

b. Specific Guidelines for Phased Array Antennas

The phased array antenna rules are established by the FCC in Title 47 of the Code of Federal Regulations Part 15, or FCC 47 CFR Part 15. Under this guideline, which was revised most recently on July 12, 2004, the narrow beams emitted by the phased array antenna are *each* considered to be an individual PTP link. The total power of the antenna system, however, cannot exceed 8 dB above 1 watt, the limit for an individual beam. Also, just as the PTP link power rules state above, the total output power must be reduced by 1 dB for each 3 dB in antenna gain above 6 dBi. These revisions to Part 15, Section 9 of the FCC Report and Order 04-165 that have been discussed read as follows:

> In addition, the Commission proposed to allow **sectorized** and **phased** array systems to operate at the **same power levels** permitted for **point-to-point directional antennas** by limiting the total power that may be applied to each individual beam to the level specified in Section 15.247(b), i.e., **0.125 watt or 1 watt, depending upon the type of modulation used**. This change implies that when operating along multiple paths, the aggregate power in all beams could exceed the output power permitted for a single point-to-point system. We proposed, therefore, to **limit the aggregate power transmitted simultaneously on all beams to 8 dB above the limit for an individual beam**. This added restriction will allow a maximum of six individual beams to operate simultaneously at the maximum permitted

[9] Carpenter and Barrett, Certified Wireless Network, 51-85.

> power. If more than six individual beams are used, then the aggregate power must be adjusted to fall within the 8 dB limit. Finally, the Commission proposed that **the transmitter output power be reduced by 1 dB for each 3 dB that the directional antenna gain of the complete system exceeds 6 dBi**. This requirement is similar to the present rules for point-to-point operation in the 2.4 GHz band (emphasis added).[10]

C. OPEN VPN TECHNOLOGY

1. Virtual Private Networks (VPN)

A VPN is exactly what it sounds like: a private network established via the Internet, which services specific users and isolates the data exchanged between these users from other users on the Internet. They can be constructed using software or a combination of hardware and software.[11]

a. Tunneling

Tunneling is the method and the meaning behind the "virtual" portion of a VPN. Just as a tunnel connects two different locations through a common path, a VPN connects users electronically and not physically, hence, the term virtually. The virtual connection between users, or clients, over the Internet can be achieved in a variety of ways. A commonly used connection method is a user at one end (of the connection) and a device that enables connectivity at the other end, such as a router or a server. This method allows multiple users to authenticate and access services or resources allowed by the VPN.

---

[10] Carpenter and Barrett, Certified Wireless Network, 85.

[11] Tamera Dean, Network+ Guide to Networks, Fourth Edition. April 4, 2005, 388-402.

b. Layer 2 OSI

Another important facet of tunneling is that it takes place at the Data Link Layer, or Layer 2 of the Open Systems Interconnection (OSI) Model for networking communications. See Table 4, where the physical packaging and transmission of network frames occurs. The tunneling protocol at the Data Link Layer encapsulates or completely encloses the higher-level protocol (Layer 3 – Network Layer) information so that it can be interpreted by a lower level. Encapsulation is like placing an envelope inside a larger envelope.[12]

OSI Model Layer	Function
Application (Layer 7)	Provides interface between applications and network for interpreting application requests and requirements
Presentation (Layer 6)	Allows hosts and applications to use a common language; performs data formatting, encryption, and compression
Session (Layer 5)	Establishes, maintains, and terminates user connections
Transport (Layer 4)	Ensures accurate delivery of data through flow control, segmentation and reassembly, error correction, and acknowledgment
Network (Layer 3)	Establishes network connections; translates network addresses into their physical counterparts and determines routing
Data Link (Layer 2)	Packages data in frames appropriate to network transmission method
Physical (Layer 1)	Manages signaling to and from physical network connections

Table 4. Functions of the OSI layers (from Network+ Guide to Networks, 4th ed.)

[12] Dean, Network+ Guide to Networks, 63.

c. SSL/TLS

The information and traffic exchanged over the VPN tunnel is encrypted. VPN software encrypts and decrypts the data transmitted between clients and must be present at both ends of the connection to establish a secure path for communications. The result is network frames, within which data resides, that are encrypted from one client to the other, or end-to-end. Clients that wish to communicate over the VPN must have the same encryption keys installed in order to properly encrypt/decrypt the information over Secure Sockets Layer and Transport Layer Security (SSL/TLS), the commercial standard for client-server encryption schemes.[13] It should be noted that the encryption occurs at Layer 4 of the OSI Model. Therefore, the encapsulated network frame at Layer 2 has already been secured by encryption at a higher level.

2. OpenVPN

OpenVPN is open source software that provides a VPN solution utilizing the technology elements outlined above. It specifically uses SSL/TLS as its encryption method. This software is utilized as the platform for the GHOSTNet application, which will be explained in more detail below.

[13] Markus Feilner, OpenVPN: Building and Integrating Virtual Private Networks: Learn how to build secure VPNs using this powerful Open Source application. November 5, 2006, 10-21.

THIS PAGE INTENTIONALLY LEFT BLANK

III. EXPERIMENT METHODOLOGY

A. TECHNOLOGY OVERVIEW

The scope of this specific research encompasses the technology related to the Vivato 802.11b/g outdoor Wi-Fi base stations, the Ruckus sectored Wi-Fi router, and the GHOSTNet application.

1. Vivato Antenna

The Vivato VP2210 outdoor Wi-Fi base station, or access point seen in Figure 1, is a phased array or smart antenna system, which utilizes six radios to electronically steer and focus narrow radio frequency (RF) beams directly to individual clients. This beam steering capability is marketed as *PacketSteering™ Technology* and is the key component that enables extended range with greater throughput than traditional wireless access points. Utilizing the 802.11g protocol, the phased array antenna base stations are capable of providing network connectivity at distances *greater* than 6,000 meters (m), which is equivalent to 3.24 nautical miles (NM), 6 kilometers (km), or 3.73 miles (mi). The antenna's wireless network coverage is approximately 100 degrees (horizontal axis arc) by 12 degrees (vertical axis arc) with data rates of up to 56 Mbps. The capable data rates are dependent upon the distance from the base station. The complete physical and technical specifications, including the detailed listing of capable data rates at designated distances from the base station, are listed in Appendix B.

Figure 1. VP2210 – Vivato Outdoor Wi-Fi Base Station. (From Vivato website)

2. Ruckus Device

The Ruckus Media Flex 2835 is a wireless router, seen in Figure 2, which utilizes a patented smart antenna system, called *BeamFlex™,* in order to maximize wireless network coverage in its immediate area, which may or may not have line of sight (LOS) with the wireless base station. The Ruckus device increases the wireless footprint of the Wi-Fi base station by providing extended range and higher data rates. The smart router system, however, must be able to associate with the wireless base station, and requires LOS to provide network coverage. The Ruckus device contains six, sectored directional antennas which automatically reconfigure themselves, in real-time, to provide the optimal wireless signal to an area of coverage equivalent to most commercial wireless routers. The device operates in two modes, bridge and router mode. In bridge mode, it acts as a wireless bridge device to connect two wired or wireless networks, or a combination of the two. In route mode, it acts as a wireless router, providing access to a wireless network that it is associated with.

Figure 2. Ruckus Media Flex 2835. (From Ruckus Website)

3. GHOSTNet

GHOSTNet is a secure, transparent, anonymous, Ethernet tunneling (OpenVPN) application. It is used to establish a secure connection by tunneling into a wired or wireless network infrastructure to communicate between other remote VPN enabled clients, or users, over untrusted and/or unsecure networks. Designed to secure communications by encrypting the information transmitted across the Internet, GHOSTNet also protects the true IP address of the client computer by making it anonymous. When GHOSTNet is enabled, the IP address reported by the client is in a completely separate physical location than the actual IP address being used by the client computer. These locations are predetermined and configured by remote servers, which enable GHOSTNet clients the attribute of anonymity. Clients wishing to establish secure communications utilizing GHOSTNet must have installed both the OpenVPN application and the GHOSTNet common keys, for encryption/decryption.

4. Testing Equipment

a. Hardware

Three laptops were used in the field testing of the Vivato–GHOSTNet Network. The laptops' specifications are as follows:

Dell© Inspiron 5100 laptop (1.0 GHz Intel Pentium II processor; 512MB RAM; and Windows XP service pack 2)

Two Apple© MacBook laptops (2.4 GHz Intel Core 2 Duo processor; 2GB RAM; Mac OS X and Windows XP service pack 2, running over VMware Fusion Virtualization software).

b. Software

Ixia IxChariot was utilized as the network packet generation and analyzing software package to conduct and document all network performance tests. IxChariot simulates real-world network traffic and applications to predict device and system performance under realistic load conditions. This software package is comprised of the IxChariot Console, which generates and analyzes network packet traffic characteristics between Performance Endpoints. For these specific field tests, the IxChariot Console was loaded onto the Dell laptop and the endpoints were loaded onto the Dell and the two Macbook laptops.

B. COASTS OVERVIEW

The Cooperative Operations and Applied Science & Technology Studies (COASTS) is an international field experimentation program designed to develop and assess Commercial Off the Shelf (COTS) and leading edge

technologies for specific military, peacekeeping and stability operations, law enforcement, and first responder missions. COASTS engages international and domestic partners at the research and development (R&D) level through cooperative science and technology field experimentation to investigate and match participant mission needs with integrated command and control, computers, communications, intelligence, surveillance and reconnaissance (C4ISR) solutions in domestic, bi-lateral and multi-national environments. COASTS conducts integrated, multi-phase scenarios to demonstrate and evaluate these C4ISR solutions over a series of five field experiments (FEX I–V), which ultimately culminate at FEX V in the final demonstration scenarios.

1. FEX-II/III

In January and February 2008, Field Exercise II and III were conducted at Camp Roberts, California, in the vicinity of McMillen Airfield. These two FEXs served as local site survey evolutions and network preparation exercises to determine requirements for FEX IV and V, the COASTS-08 final scenario and demonstrations in Thailand. McMillen Airfield's strategic location provided a chance to deploy and test realistic network topologies and link scenarios. The physical network architecture and layout that would be employed in Thailand during FEX IV and V was constructed using the runway, installations, and roads surrounding the airstrip, see Figure 3. Valuable lessons learned and network requirements were gathered from performing the

required tests on the actual equipment configurations that were planned to be demonstrated in the following months in Thailand.

Also contributing to FEX III was the United States Coast Guard (USCG), from the USCG Station Monterey Bay. The USCG provided the use of a 41-foot utility boat (UTB) for underway testing on Monterey Bay. The USCG UTB made it possible to conduct proof of concept testing for the wireless network provided by the Vivato phased array base station, Ruckus device, and GHOSTNet application. This field testing configuration would mimic the underway demonstration that would occur at FEX IV in Thailand.

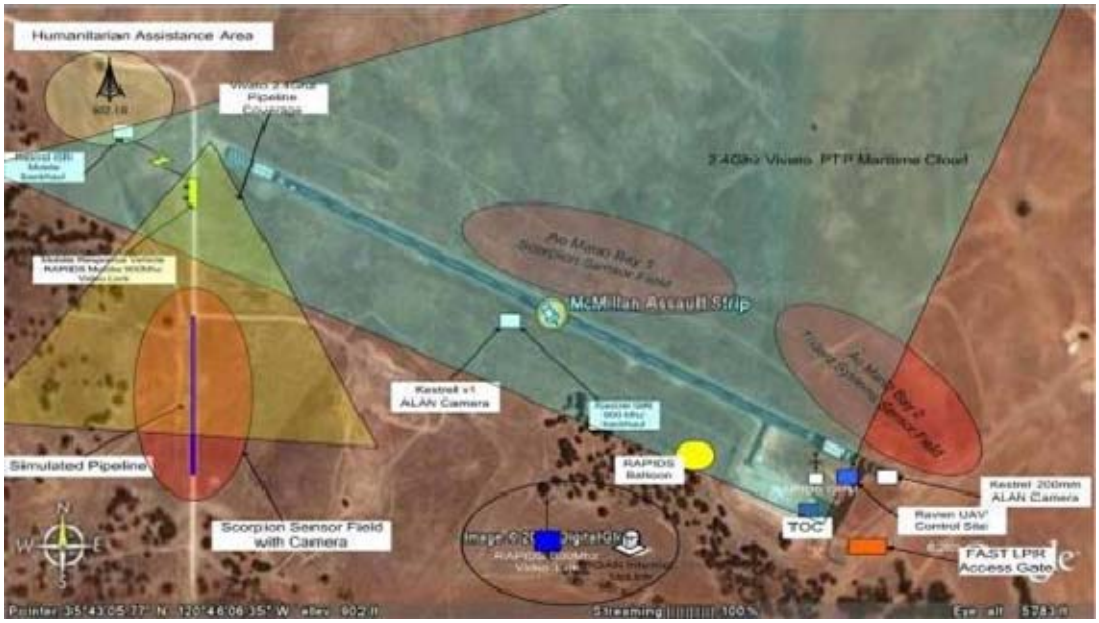

Figure 3. Network architecture for FEX II/III at Camp Roberts, CA.

2. Proof of Concept Testing – FEX III

The purpose of this preliminary phase of testing was to ensure that a basic test plan could be reasonably executed, under the reasonably moderate operating conditions of Monterey Bay, before expending time and resources on field tests in Thailand. With the assistance of USCG Station Monterey Bay, underway testing commenced on February 14, 2008, during FEX III.

a. Testing Concept of Operations (CONOPS)

The concept of the test plan was to be able to transmit data and video wirelessly from an underway vessel on Monterey Bay using the 802.11g signal provided by the phased array wireless antenna. GHOSTNet would then enable the video or data to be securely transmitted to remote locations via tunneling through the internet. Figure 4 outlines the network architecture utilized in the testing, and will be used to better illustrate the conduct of the experiment.

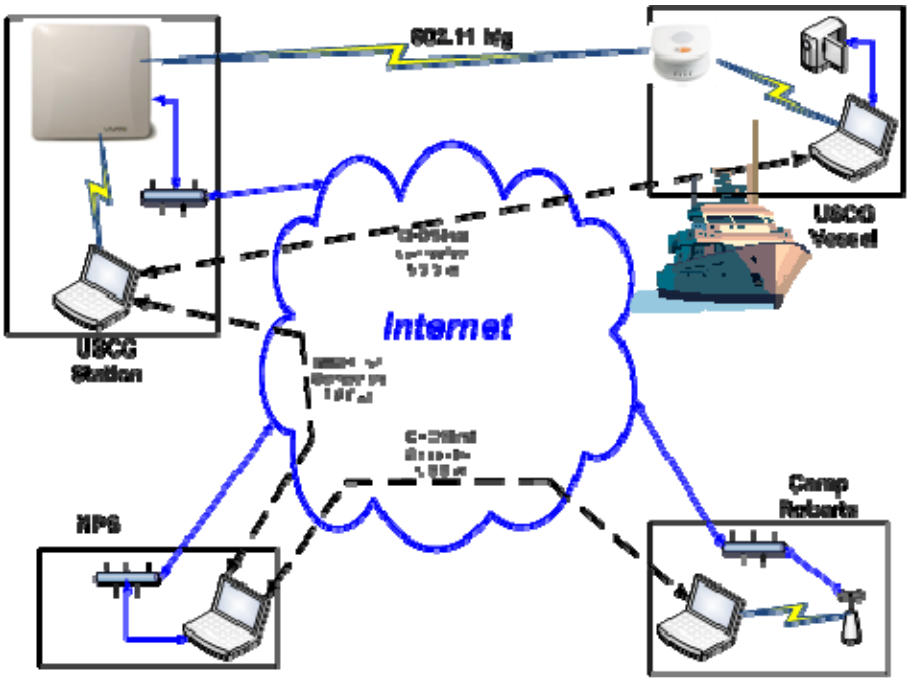

Figure 4. Proof of concept testing network architecture.

At the USCG Station, the phased array antenna, or Wi-Fi base station, was mounted overlooking Monterey Bay, at a height of eye of approximately 25 feet, seen in Figure 5. The Wi-Fi base station was connected to the USCG Station's internet service provider (ISP) via a CATEGORY 5 Ethernet cable. The Dell laptop hosting IxChariot, was wirelessly associated to the base station and served as the shore endpoint for the network performance tests run between the USCG Station and the underway vessel on Monterey Bay.

Onboard the 41-ft. USCG utility boat (UTB), which is seen in Figure 7, one of the Macbooks would serve as the underway endpoint for testing. Also aboard the UTB was a Ruckus device, or Wi-Fi router, which was mounted to the mast as seen in Figure 6, and an Axis 213 internet

protocol (IP) camera, which was configured to a Dell laptop and secured inside the pilothouse to capture and transmit video across the wireless network.

Figure 5. Phased array base station at USCG Station, Monterey Bay.

Figure 6. Ruckus device mounted to mast of USCG UTB.

Figure 7. USCG Station Monterey Bay 41-ft. utility boat.

The focus of the testing was to observe the ability to transfer data packets and provide streaming video from the underway UTB to the USCG Station ashore, and to a remote command center (JOCC on McMillen Airfield) over 100 miles away at Camp Roberts, California, seen in Figure 8.

Figure 8. Distance between Monterey Bay and Camp Robert, CA. (From Google Earth)

The execution of the test plan would encompass running network performance tests at three specific locations of the UTB while underway on Monterey Bay. As shown in Figure 9, data and video tests were conducted over the network at two, three, and four nautical miles (NM) from the USCG Station.

Figure 9. Proof of Concept testing on Monterey Bay. (From Google Earth)

b. Weather Observations

February 14, 2008, was a considerably rough day on Monterey Bay, especially underway on a 41-ft. UTB. A small craft advisory was in effect throughout the underway testing and maneuverability for optimal testing was limited. The UTB experienced swells of 5–8 ft., which impacted the conduct of testing, and will be discussed in greater detail in section VI, Results and Analysis.

3. FEX-IV/V

Field Exercise IV and V, conducted in March and May 2008 respectively, took place at Ao Manao Airbase near Prachuap Khiri Khan, Thailand seen in Figure 10. Ao Manao is located approximately 312 km, or 194 miles, south of Bangkok. All successful implementations of test equipment and experiments at FEX II and III would be deployed at Ao Manao for further operational testing and development. For the Vivato–GHOSTNet wireless network specifically, FEX IV and V would be utilized to tie together previous network tests conducted at Monterey Bay and Camp Roberts.

Figure 10. GPS location of network performance tests conducted during FEX IV. (From Google Earth)

a. Scope of the Field Testing

The intent of the Vivato–GHOSTNet testing was to demonstrate the feasibility of utilizing an 802.11g network over water and land in order to provide secure Global Data Dissemination (GD^2) to physically remote operational commanders and their staff. From a remote C^2 center, the planning staff and/or COC would have the ability to view and

receive video, voice, and data from a naval unit conducting a maritime interdiction operation (MIO) boarding on an underway vessel.

b. Measures of Effectiveness and Performance

The COASTS-08 Field Exercises provided an environment in which to test the qualitative measurements of the Vivato–GHOSTNet Network. The Measures of Performance (MOPs) directed that bandwidth and throughput performance of a network were the most important factors for testing. The qualitative measures were formed by reviewing the COASTS-06 and COAST-07 after action reports (AARs) that showed considerable network degradation during high bandwidth usage and video streaming evolutions.

For the Measures of Effectiveness (MOE), Ixia's IxChariot was implemented to collect, display, and analyze the pertinent information related to network performance characteristics, which will be discussed in the sections below. The raw test data was collected and downloaded into two common file formats, 'csv' and 'html.'

c. Selected Measures (Metrics)

The metrics used for these tests were: *throughput*—as measured by bulk transport capacity; *response time*—as measured by roundtrip delay and loss; and *video streaming*—as measured by throughput thresholds on video packets and the ability to view video free of hesitation, or visually delayed motion.

(1) ***Throughput*** measures the maximum amount of *intended* data transferred across a communications link

or network. It does not include any additional packets or encryption overhead, which may be transferred due to strong encryption schemes implemented or multiple data transmissions over the wireless medium, which would constitute the total data rate. The method used to perform this measurement is to transfer a file of approximately 30,000 bytes between two network nodes and measure the time taken to receive the file without errors. The throughput is then calculated by dividing the file size by the time to get the intended data in megabits per second (Mbps).

(2) ***Response Time*** is a measure of effectiveness related to the amount of time it takes a data packet to traverse a given distance. Essentially, it is the elapsed time between the end of an inquiry on a computer system and the beginning of a response. Network performance monitoring tools were configured to measure and display various parameters characterizing communications between or among a pair of network endpoints, or nodes. In TCP/IP-based networks, one such parameter was the network Round Trip Time (RTT). As a control measure, the RTT was measured from the shore-based endpoint location, which initiated IxChariot performance tests, to eliminate any inconsistencies related to tests taken at various locations.

(3) ***Video Streaming*** refers to the ability of an application to play synchronized video media streams, in a continuous way, while they are being transmitted to the client over a data network.

d. FEX IV Field Testing CONOPS

Three phased array antennas were mounted on a communications tower (Comms Tower) approximately 150 ft. high, seen in Figure 11. The antennas were orientated on the tower to cover the north, south, and west sectors respectively. The 100-degree horizontal arc of coverage of each antenna provided overlap coverage for testing over land and underway in the vicinity of Ao Manao, as shown in Figure 12.

Figure 11. Phased array antennas mounted on Comms Tower on Ao Manao Airbase in Thailand.

Figure 12. 802.11g wireless coverage sectors by Vivato antennas mounted on Comms Tower. (From Google Earth)

Multiple iterations of endpoint tests were conducted utilizing the three antennas mounted on the Comms Tower. The endpoint tests were initiated from the shore endpoint, the Dell laptop with IxChariot, to the remote endpoint, the Macbook, whether it was over land, over water, or underway on the north or south bay.

Underway testing was conducted onboard a Royal Thai Navy (RTN) Fast Patrol Craft (PCF), seen in Figure 13. The PCF was 19.6m (64.3 ft.) in length, 5.3m (17.4 ft.) in

width, and had a draft of 2.85M (9.3 ft.). The configuration of sensors was nearly identical to that of the USCG UTB in Figure 4. The RTN PCF was loaded out with a Ruckus mounted to the mast, a Macbook onboard as the (remote) network testing endpoint, and an IP camera to capture video to be transmitted to remote viewers via the wireless network. The streaming video captured onboard the PCF was viewed at the Joint Operations Command Center (JOCC) on Ao Manao Airbase and at NPS in Monterey, California, via the Vivato–GHOSTNet network. Testing also took place at the PCF pier, seen in Figure 13 and 14, and underway in the south bay at various distances.

Figure 13. Royal Thai Navy PCF pierside in Prachuap Khiri Khan, Thailand.

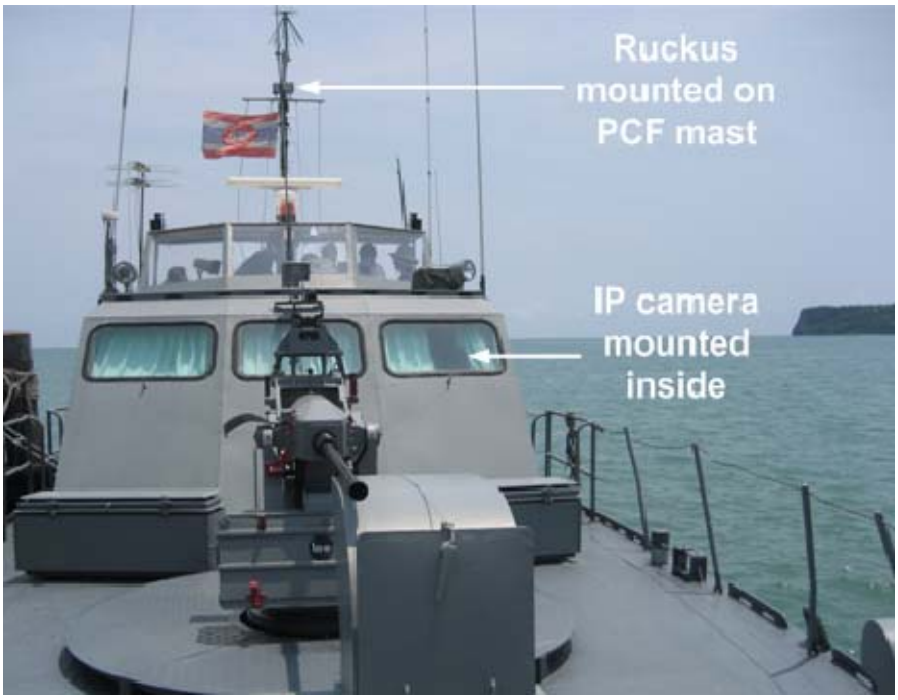

Figure 14. Testing device configuration onboard RTN PCF, for FEX IV testing in Thailand.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESULTS AND ANALYSIS

A. PROOF OF CONCEPT TESTING

On February 14, 2008, the day of testing, a small craft advisory was issued for Monterey Bay. Four total test runs, from three locations, were completed and the results are displayed in Table 5.

Distance from Vivato antenna	Swells Observed	Round Trip Time (avg.)	% Packet Loss	Stream Video
2 NM	5 ft.	23 ms	0 %	n/a
3 NM	8 ft.	22 ms	33 %	Yes
4 NM	8 ft.	8.5 ms	16 %	n/a
2 NM	6 ft.	19 ms	37 %	Yes

Table 5. Results of proof of concept testing underway on Monterey Bay – February 14, 2008.

1. Environmental Impact

The large swells encountered on the bay by the UTB during proof of concept testing proved to be significant limitations in the completion of the evolution. The performance limitations of the wireless network included the height of the swells, which impeded the line of sight (LOS) between the Ruckus device (mounted to the UTB mast) and the phased array antenna (mounted at USCG Station). Following the 3 NM test, the Ruckus device ceased to operate, and was secured after it experienced seawater intrusion due to sea swells which contacted the mast and the pilothouse of the UTB.

The Macbook, on the UTB, maintained wireless association with the phased array antenna throughout the underway testing. Due to technical difficulties not related to the environmental factors, IxChariot endpoint tests were unable to be accomplished. Simple ping tests using the command prompt were substituted to gather some meaningful form of data transfer capability over the wireless network. Streaming video from the IP camera was successfully observed, at 2 and 3 NM tests, from the Dell laptop at the USCG Station and a Dell laptop at McMillen Airfield on Camp Roberts, California, via the GHOSTNet application.

More complete weather data for this testing evolution is located in Appendix A.

2. Observations from testing on Monterey Bay

Given the environmental impact and technical difficulties encountered during the conduct of the underway proof of concept testing on Monterey Bay, there were several important takeaways from this experiment.

a. Underway Data Transfer Capability

The ability to wirelessly transmit and receive data packets from up to 4 NM from the shore-mounted phased array antenna was demonstrated. This was performed without the use of the Ruckus wireless router, which means that the shore-based antenna was communicating with a laptop, underway on a vessel, via a wireless association to its network.

b. Underway Streaming Video Capability

Streaming video from the UTB was successfully observed at a distance of 2 and 3 NM from the (shore mounted) antenna. Utilizing GHOSTNet, this video was able to be securely viewed by multiple remote C^2 centers including the USCG Station, NPS, and Camp Roberts.

B. FEX IV TESTING – THAILAND

1. Environmental Impact

Field Testing conducted over land and water (on the PCF) was conducted on March 24 and 25, 2008. With the exception of a thunderstorm mid-day on March 25, visibility was approximately four miles and relative humidity averaged 90% for both days. The high and low temperatures recorded for March 24 were 96 and 76 degrees Fahrenheit and 91 and 77 degrees Fahrenheit for March 25. The storm on March 25 was accompanied by rough seas, wind gusts, and heavy rain in the vicinity of Prachuap Khiri Khan and Ao Manao Airbase. This was significant because due to this storm, the PCF was unable to get underway and remained made-up alongside the pier with storm lines. Although the PCF was pierside, and in spite of the dense rain, network test runs were carried out and successfully completed during the storm. Six distinct groups of tests were completed over the two-day field testing period. A more complete historical weather data for the two days is located in Appendix A.

2. Field Test Conduct

Figure 15. GPS plots of field testing locations IVO Ao Manao, Thailand. (from Google Earth)

a. Test Group 1 – Baseline

The first group of network test runs were executed in order to establish a baseline for the Vivato-GHOSTNet network. Results enabled the performance of the network to be measured without any users or encryption on the network. Endpoint 1 initiated and documented all end-to-end tests and was connected to the three phased array antennas mounted on the Comms Tower (11°47′10.71″N/099°48′34.25″E) via CAT5 Ethernet cable. The location of endpoint 1, at the Comms

Tower, was constant throughout the two day testing evolution. Endpoint 2, the remote endpoint, was located in the hanger bay (11°47’12.79”N/099°48’29.05”E) approximately 0.11 miles (0.10 NM) to the west of the Comms Tower for baseline tests, see Figure 15.

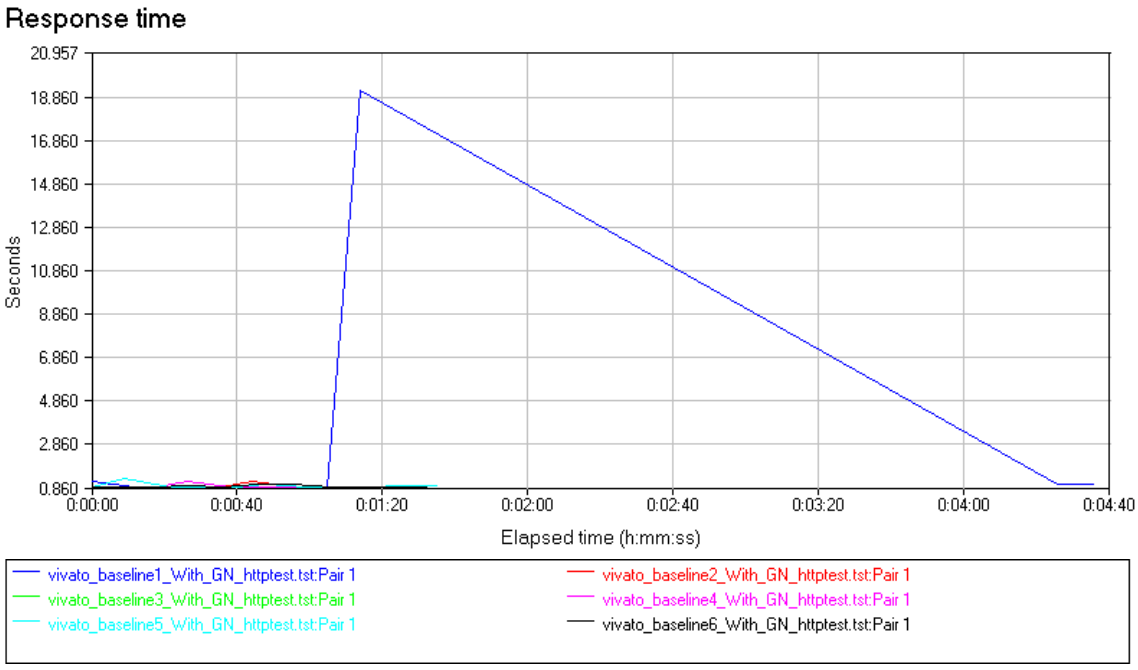

Figure 16. Response Time baseline with GHOSTNet enabled.

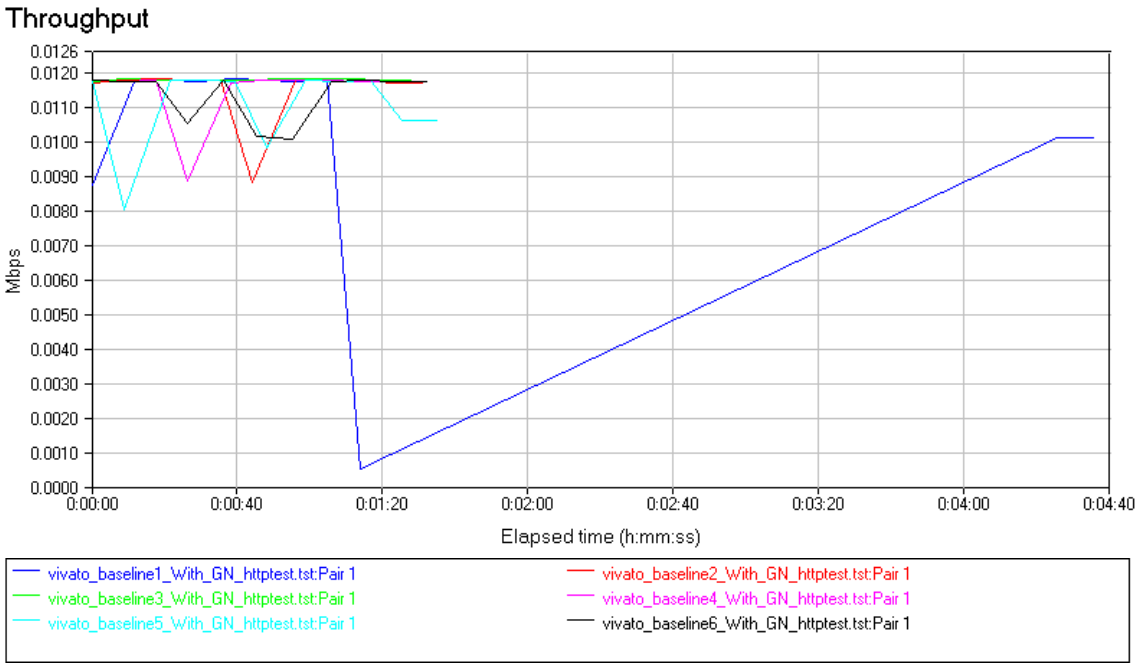

Figure 17. Throughput baseline with GHOSTNet enabled.

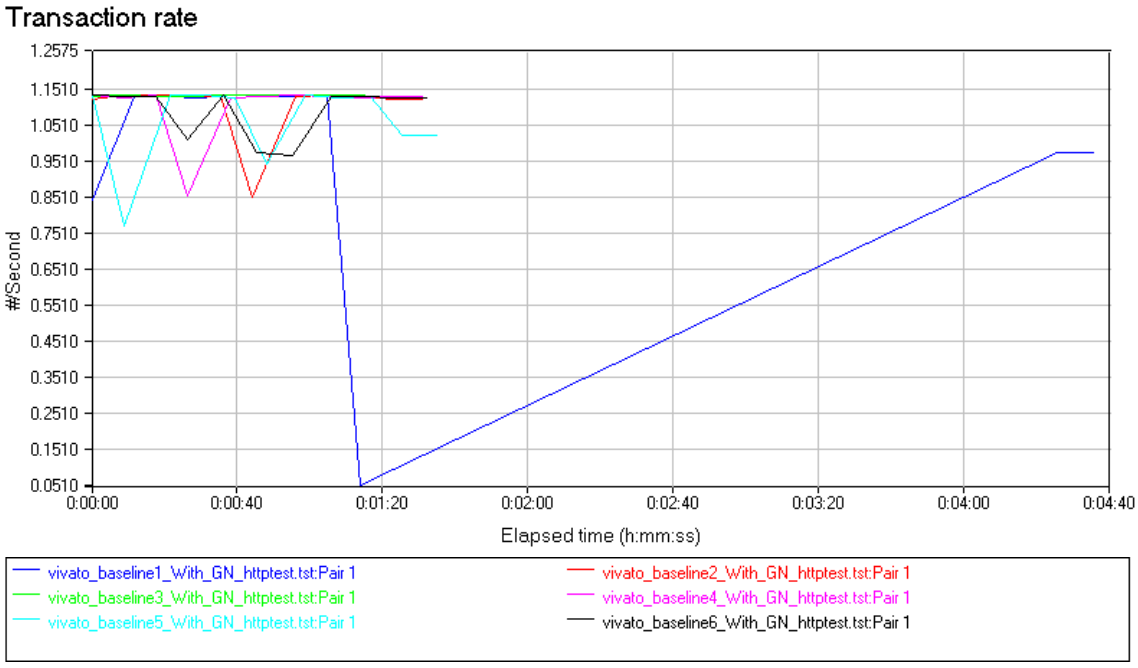

Figure 18. Transaction Rate baseline with GHOSTNet enabled.

From Figures 16–18, baseline test runs with GHOSTNet enabled, the outlier (test run one) was discarded for the purpose of analysis. The average Response Time of the five test run groups was 0.916 seconds, including a minimum time of .880 seconds a maximum time of 1.176 seconds. The average Throughput measured was 0.011 Mbps, with a minimum value of 0.008 Mbps and a maximum of 0.012 Mbps. The average Transaction Rate recorded was 1.092 transactions per seconds with a minimum rate of 0.850 per second and a maximum rate of 1.137 per second.

In the next set of test runs, GHOSTNet *was disabled* and produced the results seen in Figures 19–21. Two outliers in this group of test runs were excluded (test runs two and three) for the purpose of analysis. The average Response Time was 0.031 seconds with a minimum time of seconds and a maximum of time of seconds. The average Throughput measured was 0.360 Mbps with a minimum throughput of 0.026 Mbps and a maximum throughput of 2.364 Mbps. The average Transaction Rate measured was 34.663 transactions per second with a minimum rate of 2.501 per second and a maximum rate of 227.273 per second.

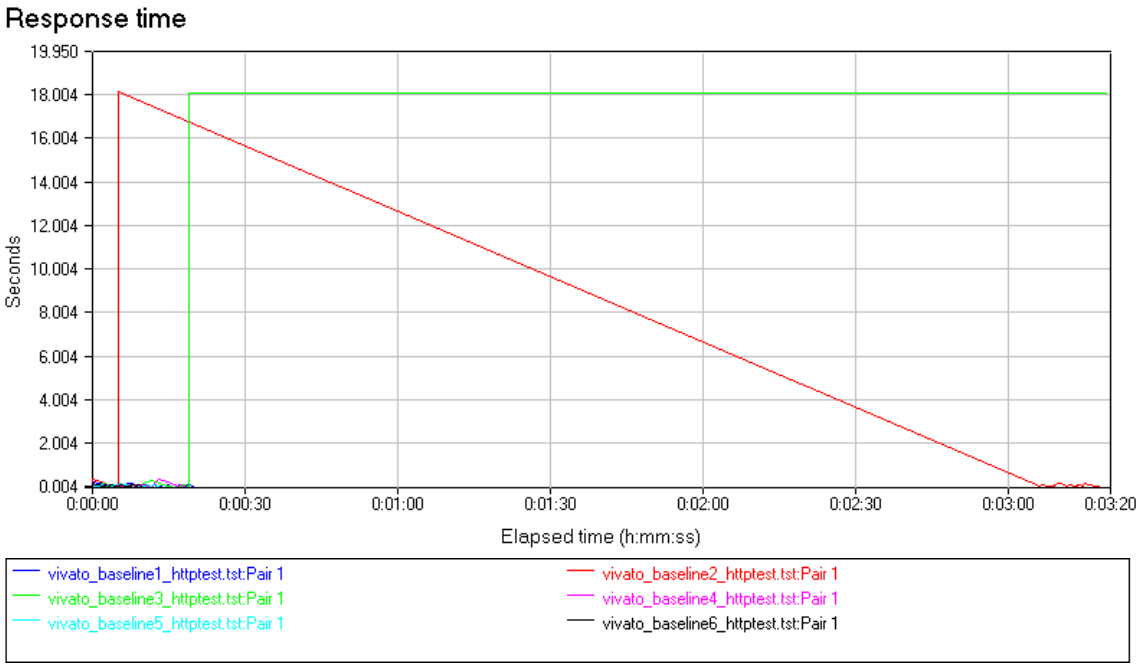

Figure 19. Response Time baseline without GHOSTNet.

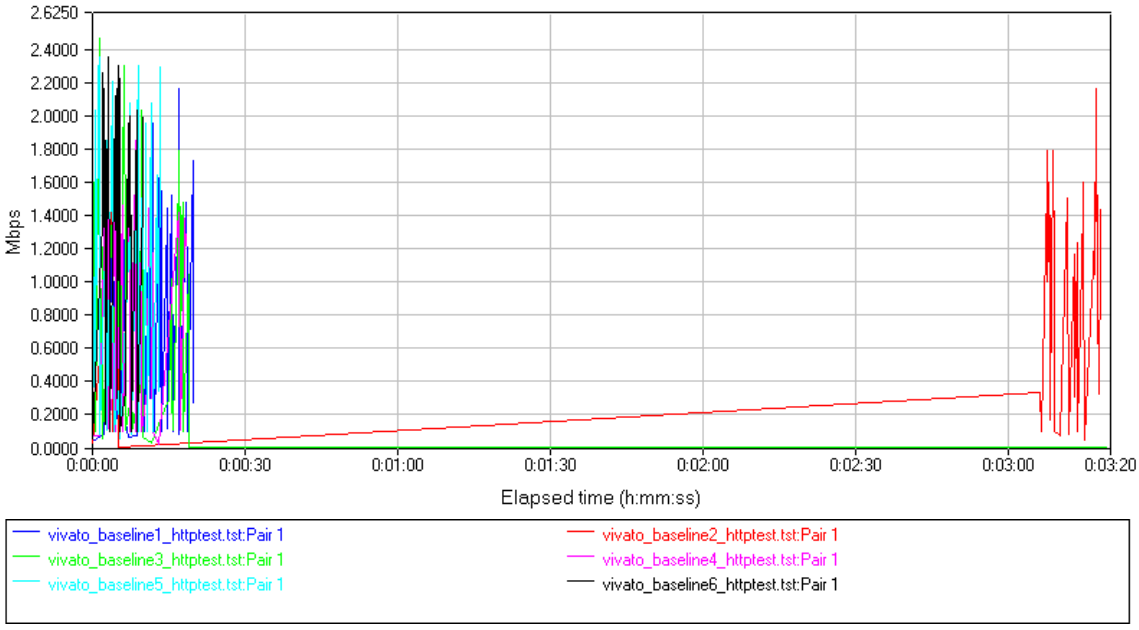

Figure 20. Throughput Baseline without GHOSTNet.

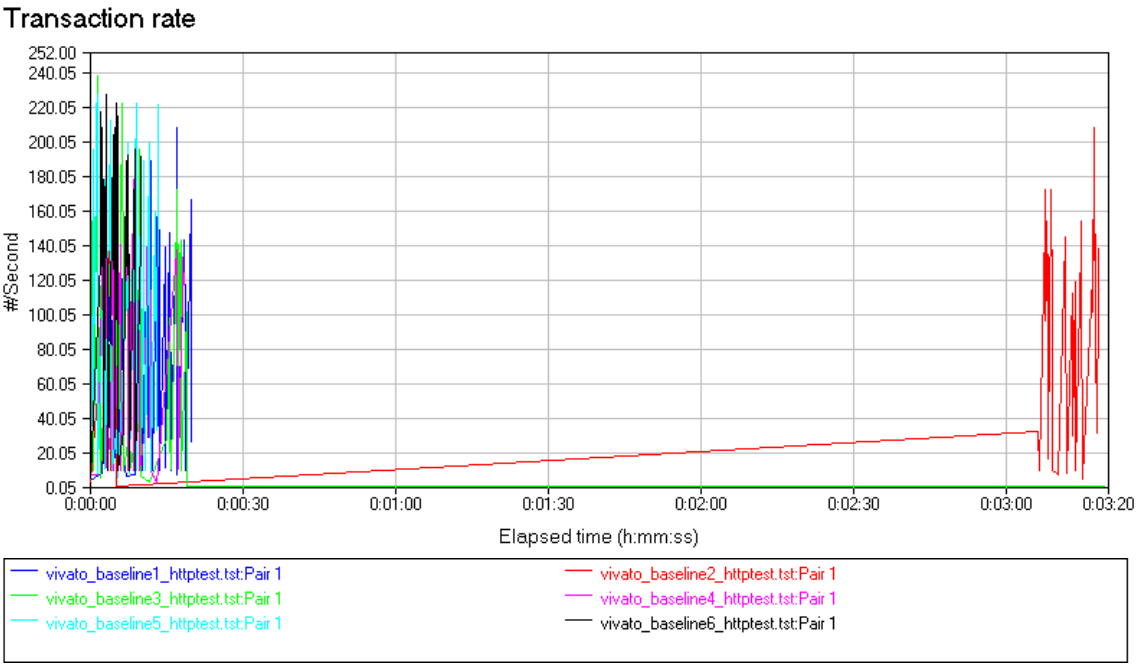

Figure 21. Transaction Rate Baseline without GHOSTNet.

b. Test Group 2 – Prachuap Beach Hotel

The second group of tests was conducted between endpoint 1 (Comms Tower) and endpoint 2, which was located on the sixth floor observation deck of the Prachuap Beach Hotel, on the north bay in Prachuap Khiri Khan, shown in Figure 22 (11°48’08.84”N/099°47’58.57”E). The distance between the endpoints for this set of tests was 1.29 miles (1.12 NM).

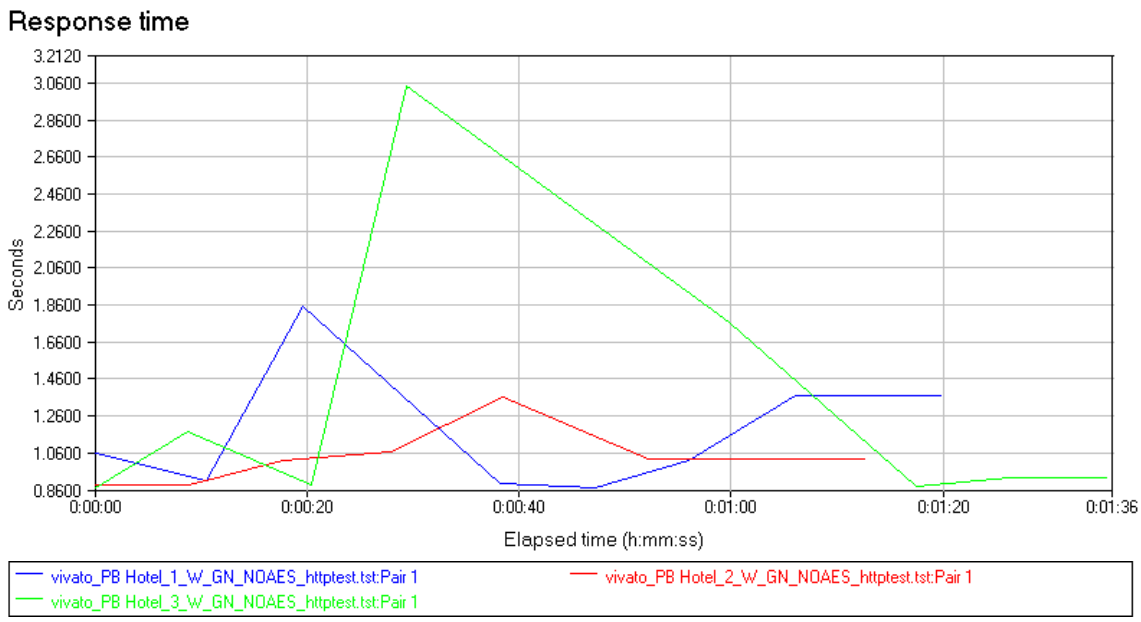

Figure 22. Prachuap Beach Hotel Response Time with GHOSTNet enabled.

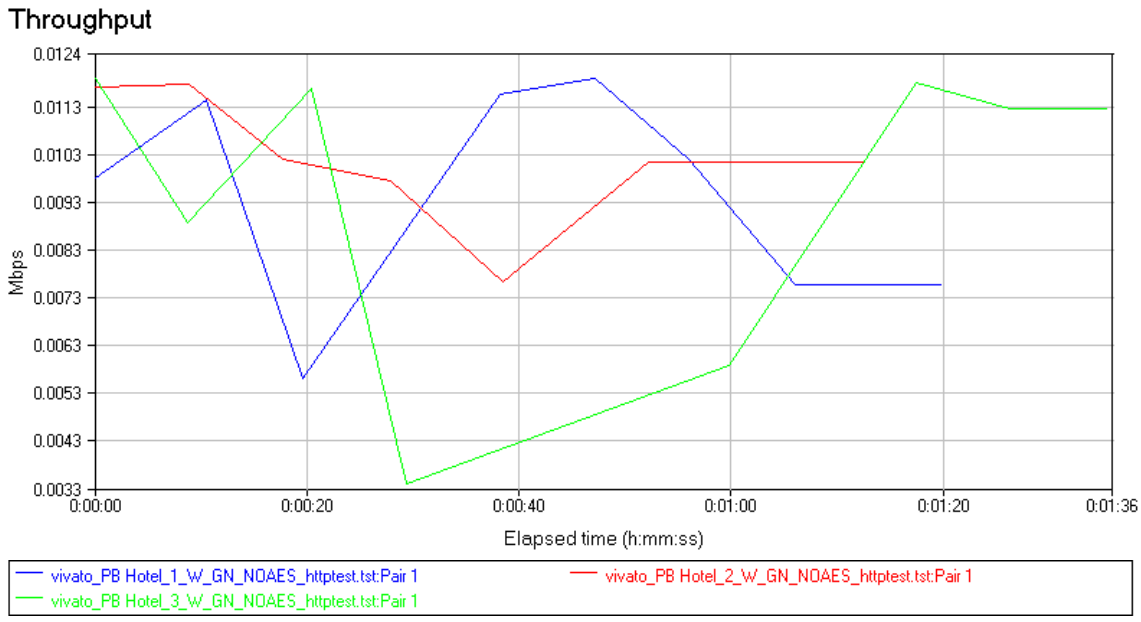

Figure 23. Prachuap Beach Hotel Throughput with GHOSTNet enabled.

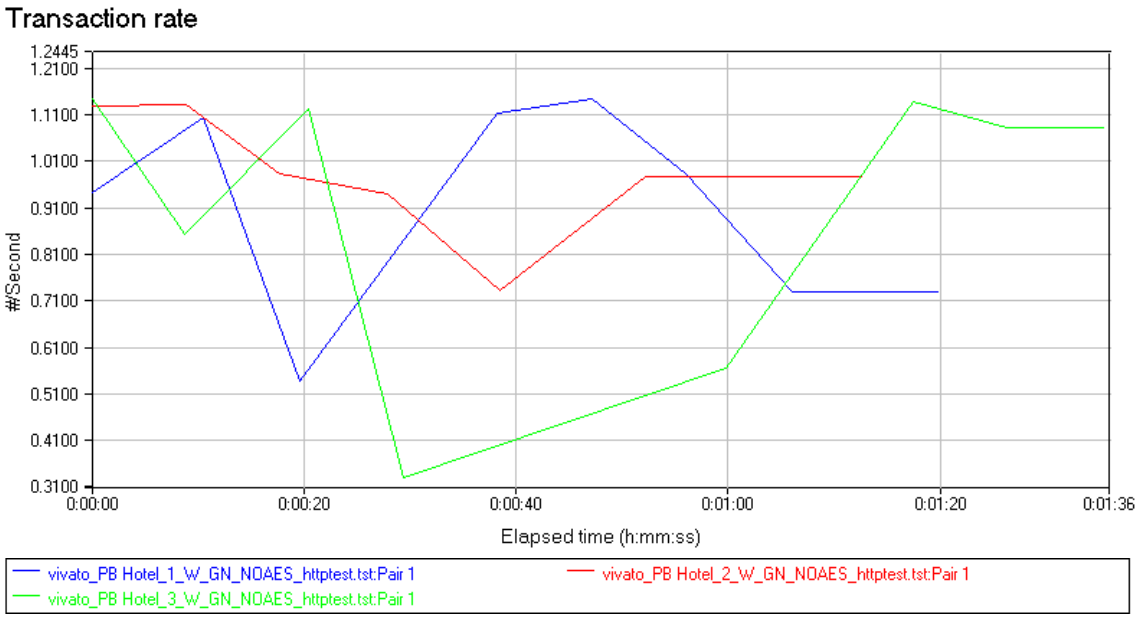

Figure 24. Prachuap Beach Hotel Transaction Rate with GHOSTNet enabled.

From Figures 22–24, the average Response Time with GHOSTNet enabled measured 1.181 seconds with a minimum time of 0.874 seconds and a maximum time of 3.041 seconds. The average Throughput measured was 0.009 Mbps with a minimum of 0.003 Mbps and a maximum of 0.012 Mbps. The average Transaction Rate measured was 0.858 transactions per second with a minimum rate of 0.329 per second and a maximum rate of 1.144 per second.

In Figures 25–27, with GHOSTNet *disabled,* two outliers (test runs four and six) excluded from the analysis. The average Response Time measured was 0.026 seconds with a minimum time of .005 seconds and a maximum time of 0.894 seconds. The average Throughput measured was 0.402 Mbps with a minimum of 0.029 Mbps and a maximum of

1.962 Mbps. The average Transaction Rate measured was 38.732 transactions per second with a minimum rate of 2.804 per second and a maximum rate of 188.679 per second.

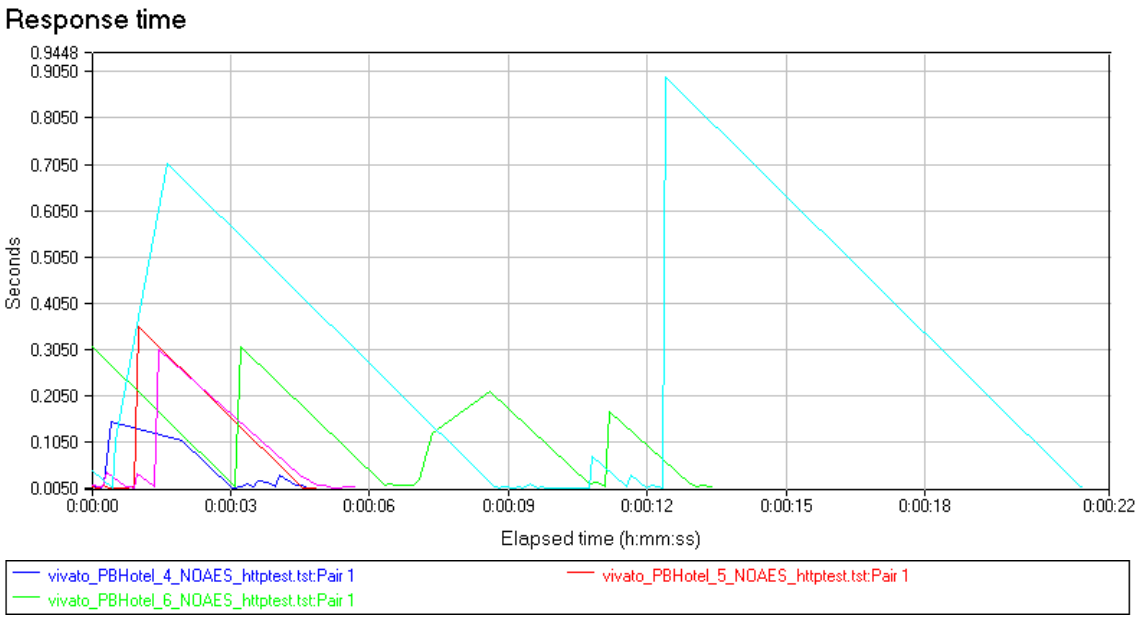

Figure 25. Prachuap Beach Hotel Response Time without GHOSTNet.

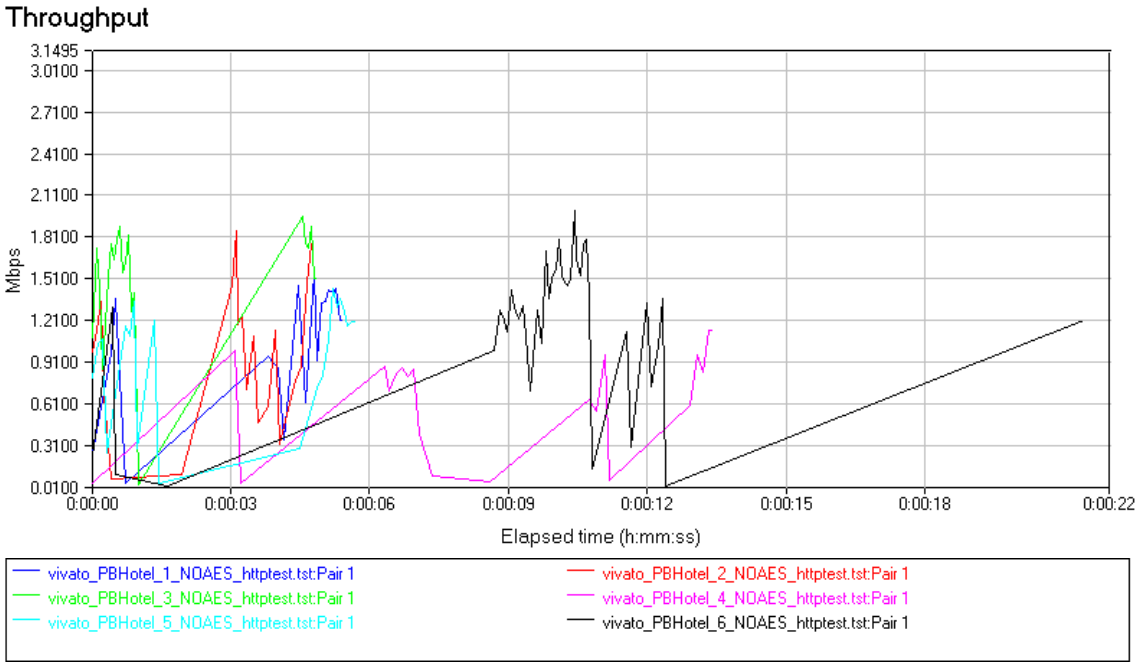

Figure 26. Prachuap Beach Hotel Throughput without GHOSTNet.

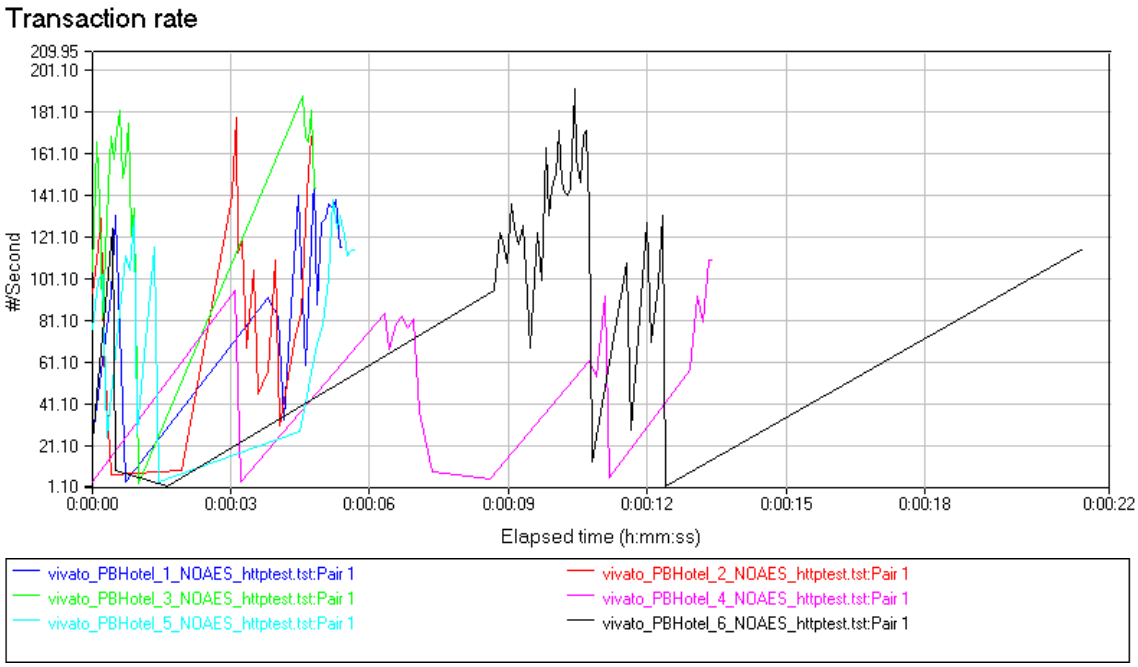

Figure 27. Prachuap Beach Hotel Transaction Rate without GHOSTNet.

c. Test Group 3 – PCF Underway at 1NM

The first underway test conducted between endpoint 1 (Comms Tower) and endpoint 2 on the PCF (11°46’32.90”N/ 099°48’43.30”E) while underway in the south bay, see Figure 11 above. The PCF was approximately 0.66NM away from the Comms Tower during the conduct of the testing. Three attempts were made to execute end-to-end tests from this location, but all test runs timed out prior to completion and no data was recorded. Testing from one nautical mile underway was secured and the PCF moved out to the two nautical mile location to proceed with testing.

d. Test Group 4 – PCF Underway at 2NM

The fourth group of test runs was conducted between endpoint 1 (Comms Tower) and endpoint 2 located

onboard the PCF (11°45’27.94”N/099°49’06.09”E), underway in the south bay 2 NM south-southeast of the communication tower. Due to underway time restrictions, testing was only conducted with GHOSTNet disabled. Further testing was conducted with GHOSTNet enabled while the PCF was pierside, see test six below. Two of the test runs (runs one and two) were significant outliers and were excluded from the analysis.

Interpreted from the four acceptable test runs seen in Figures 28–30, the average Response Time with GHOSTNet disabled was 12.998 seconds with a minimum time of 7.355 seconds and a maximum time of 37.347 seconds. The average Throughput measured was 6.155 Mbps with a minimum of 2.142 Mbps and a maximum of 10.877 Mbps. The average Transaction Rate measured was 0.077 transactions per second with a minimum rate of 0.027 per second and a maximum rate of 0.136 per second.

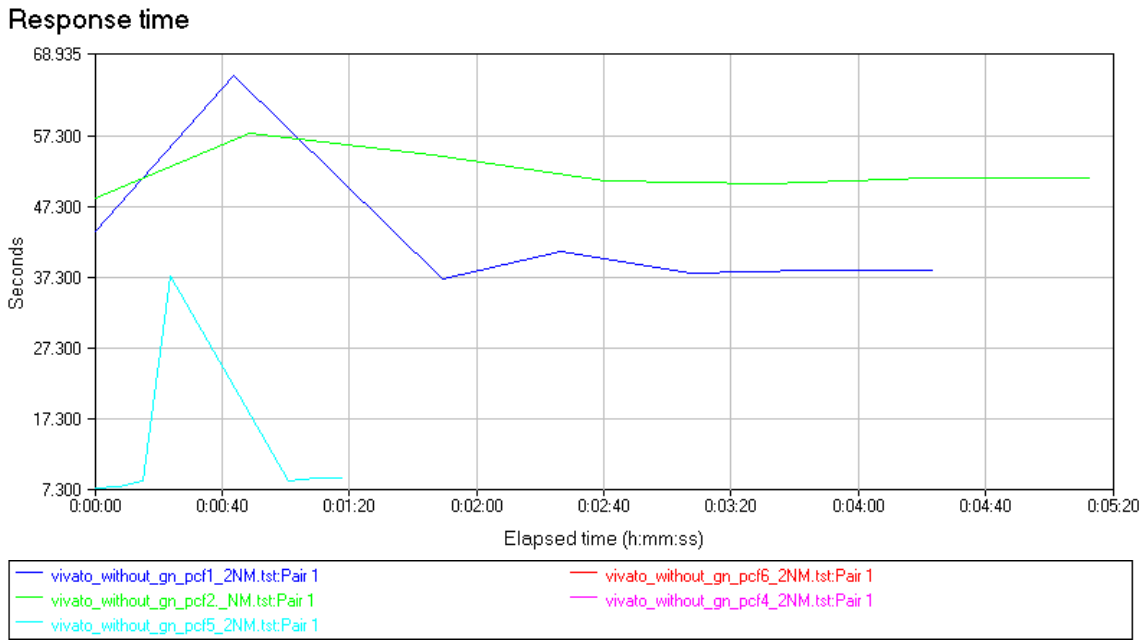

Figure 28. PCF underway at 2 NM without GHOSTNet.

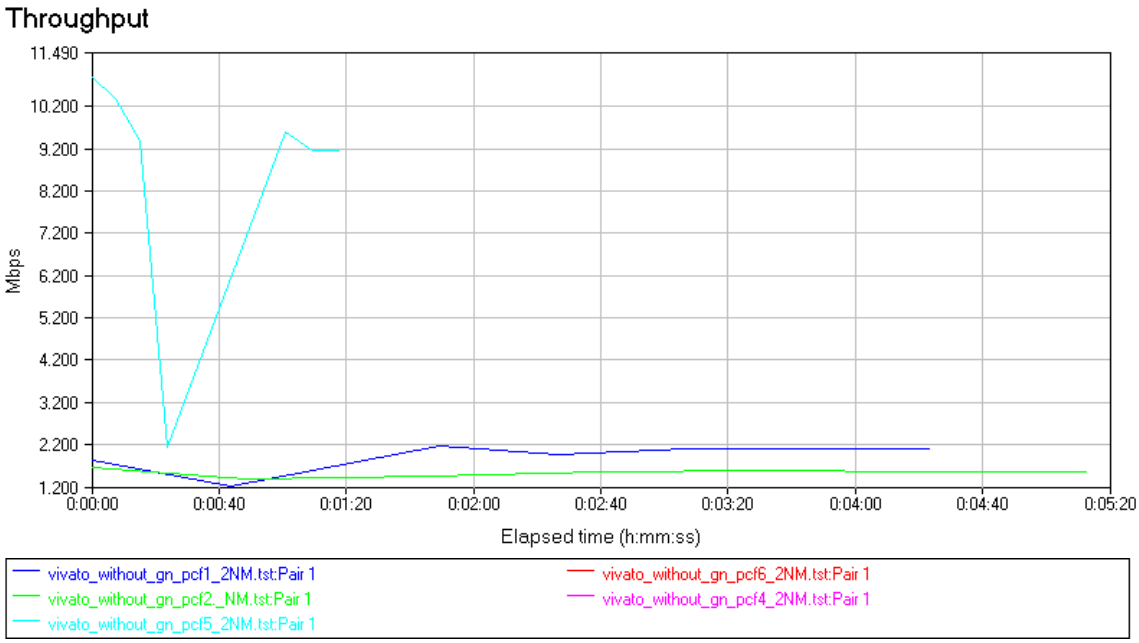

Figure 29. PCF underway at 2NM without GHOSTNet.

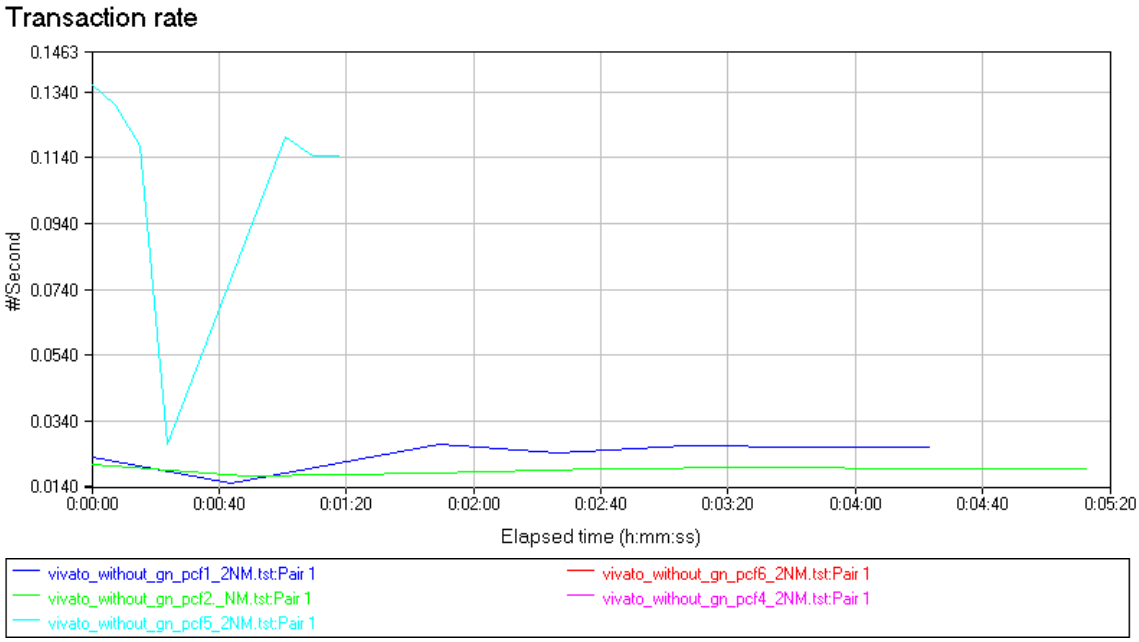

Figure 30. PCF underway at 2NM without GHOSTNet.

e. Test Group 5 – Ao Manao Hotel/BOQ

The fifth group of tests were conducted between endpoint 1 (Comms Tower) and endpoint 2 located on the fourth floor roof access at the Ao Manao Hotel/BOQ (11°46’35.21”N/ 099°47’50.38”E), seen in Figure 15, on the south bay. The distance between the endpoints was 0.93 NM.

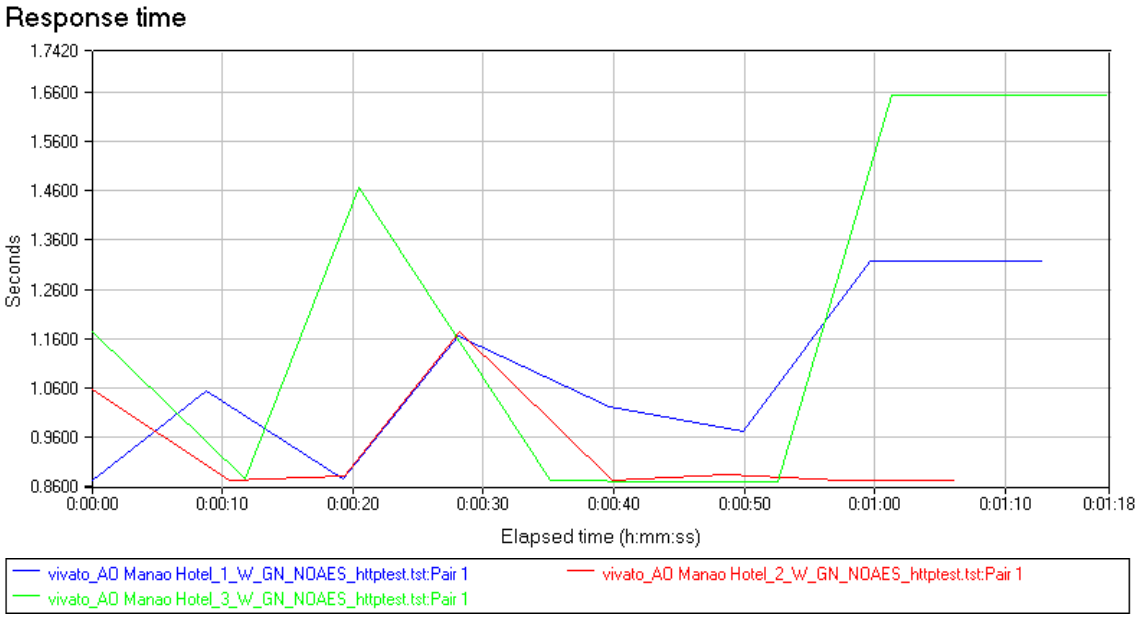

Figure 31. Ao Manao Hotel Response Time with GHOSTNet enabled.

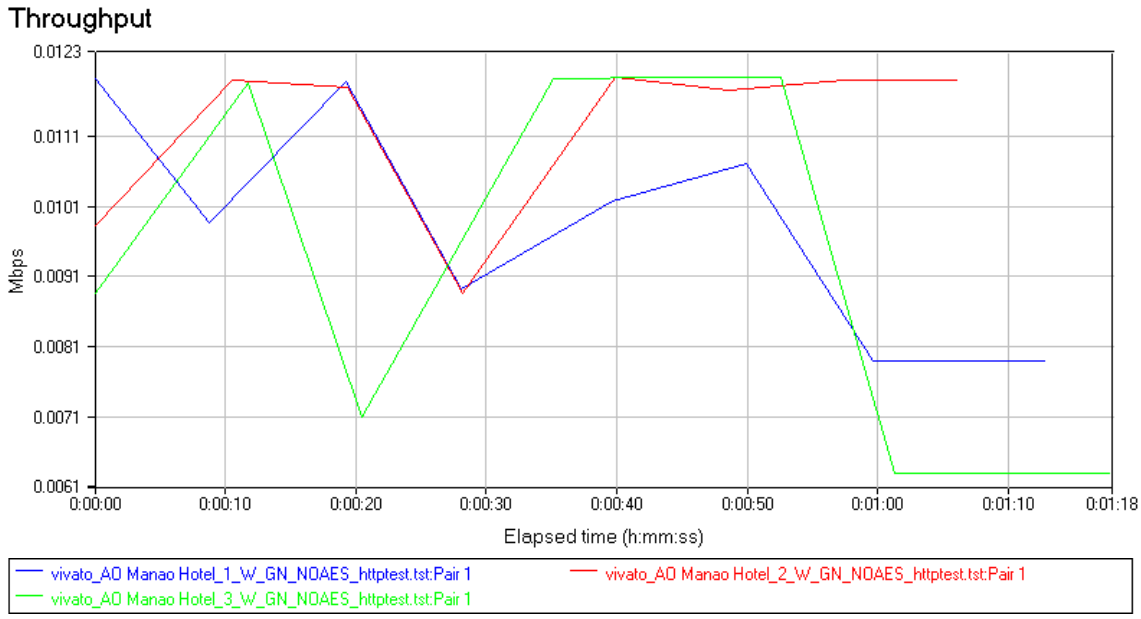

Figure 32. Ao Manao Hotel Throughput with GHOSTNet enabled.

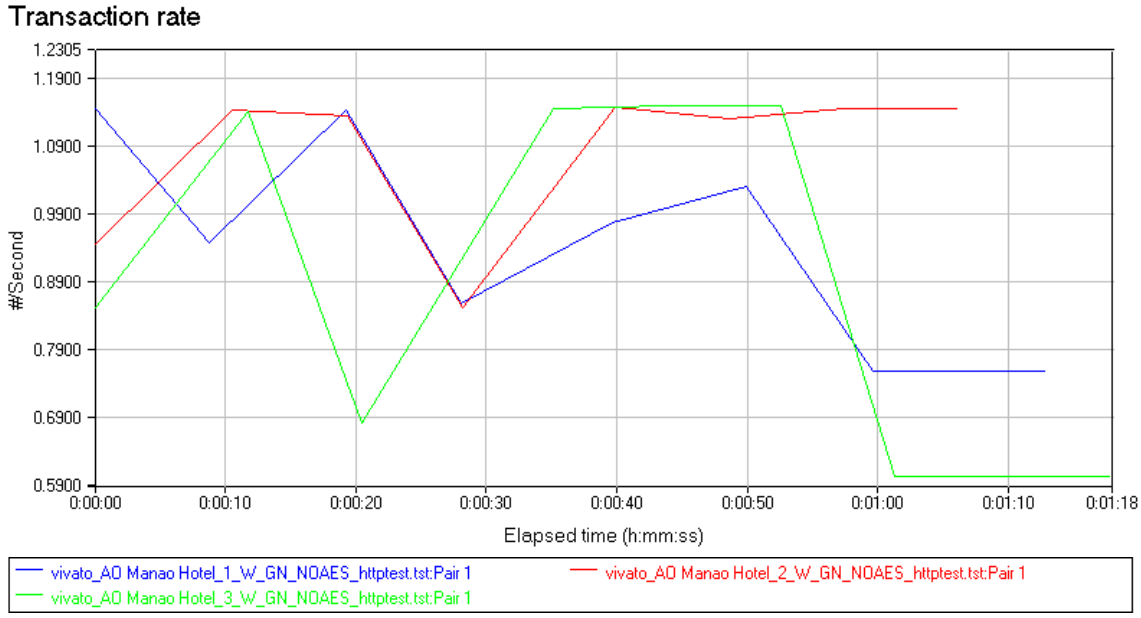

Figure 33. Ao Manao Hotel Transaction Rate with GHOSTNet enabled.

From Figures 31–33, the average Response Time with GHOSTNet enabled was 1.0327 seconds with a minimum time of 0.871 and a maximum time of 1.653 seconds. The average

Throughput measured was 0.010 Mbps with a minimum of 0.006 Mbps and a maximum of 0.012 Mbps. The average Transaction Rate measured was 0.973 transactions per second with a minimum rate of 0.605 per second and a maximum rate of 1.148 per second.

As seen in Figures 34–36, the average Response Time measured with GHOSTNet disabled was 0.670 seconds with a minimum time of 0.055 seconds and a maximum time of 18.904 seconds. The average Throughput measured was 0.137 Mbps with a minimum of 0.001 Mbps and a maximum of 2.60 Mbps. The average Transaction Rate measured was 13.256 transactions per second with a minimum rate of 0.053 per second and a maximum rate of 243.902 per seconds.

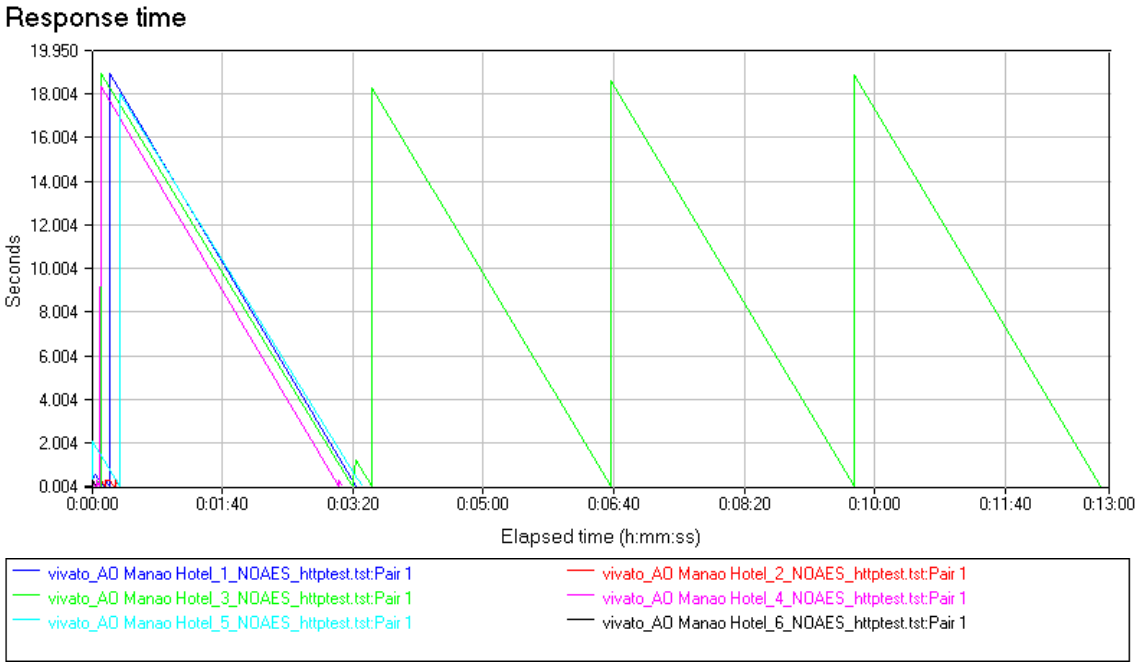

Figure 34. Ao Manao Hotel Response Time without GHOSTNet.

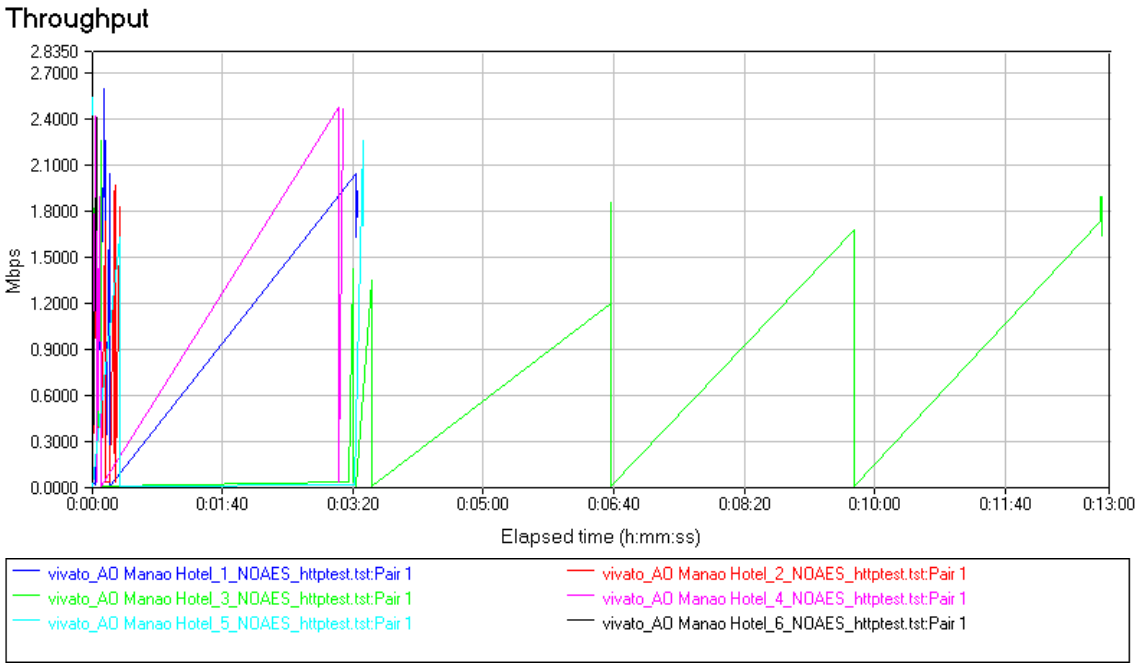

Figure 35. Ao Manao Hotel Throughput without GHOSTNet.

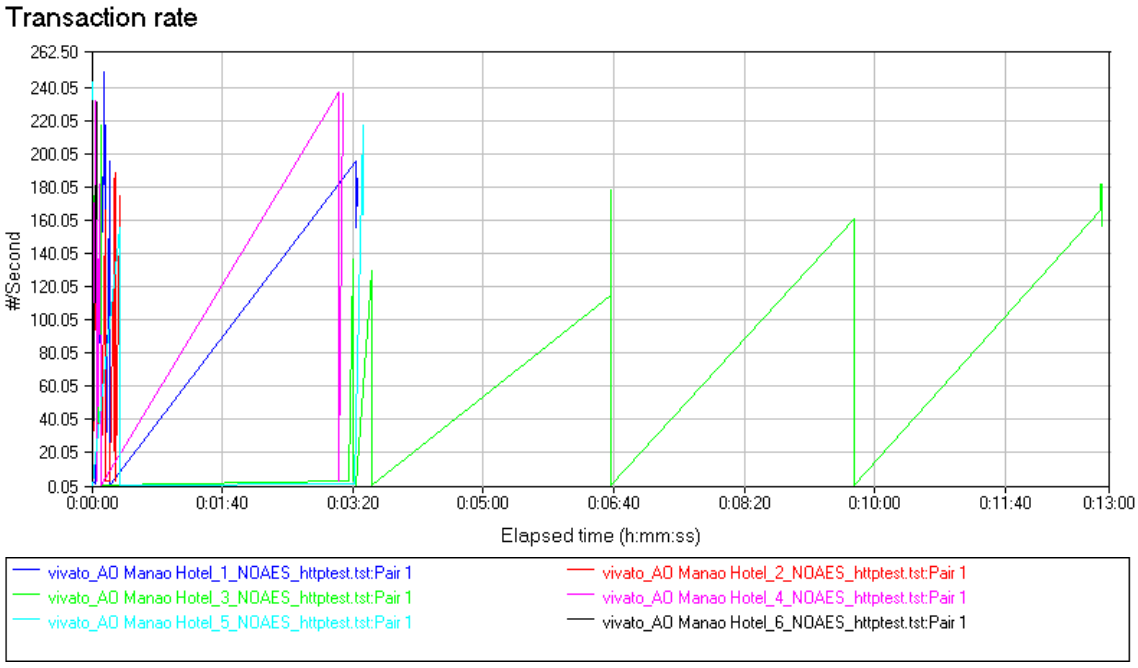

Figure 36. Ao Manao Hotel Transaction Rate without GHOSTNet.

f. Test Group 6 – PCF Pierside

The sixth group of test runs was conducted between endpoint 1 (Comms Tower) and endpoint 2 onboard the PCF pierside (11°48’29.33”N/099°48’09.02”E) in the north bay, seen in Figure 15. The intent of this testing was to conclude the underway tests with GHOSTNet enabled, however due to weather restrictions the PCF was forced to remain pierside and rig storm lines to ride out the storm. This group of tests, with the PCF pierside, was especially challenging to complete due to taller vessels, moored on the opposite side of the pier, obstructing the LOS between the PCF and Comms Tower.

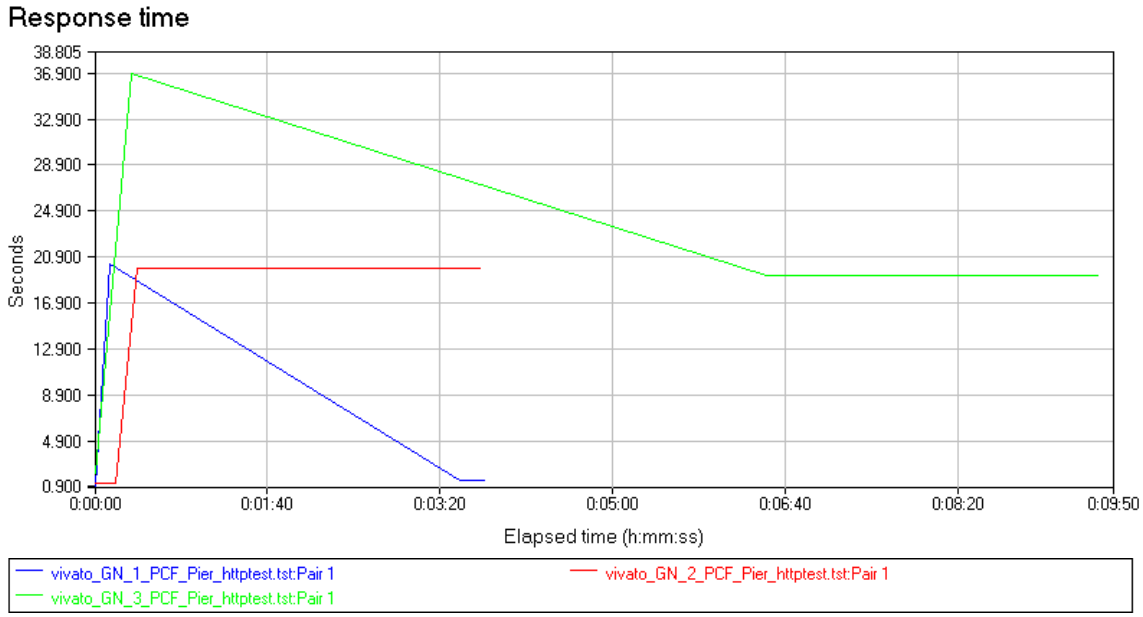

Figure 37. Pierside Response Time with GHOSTNet enabled.

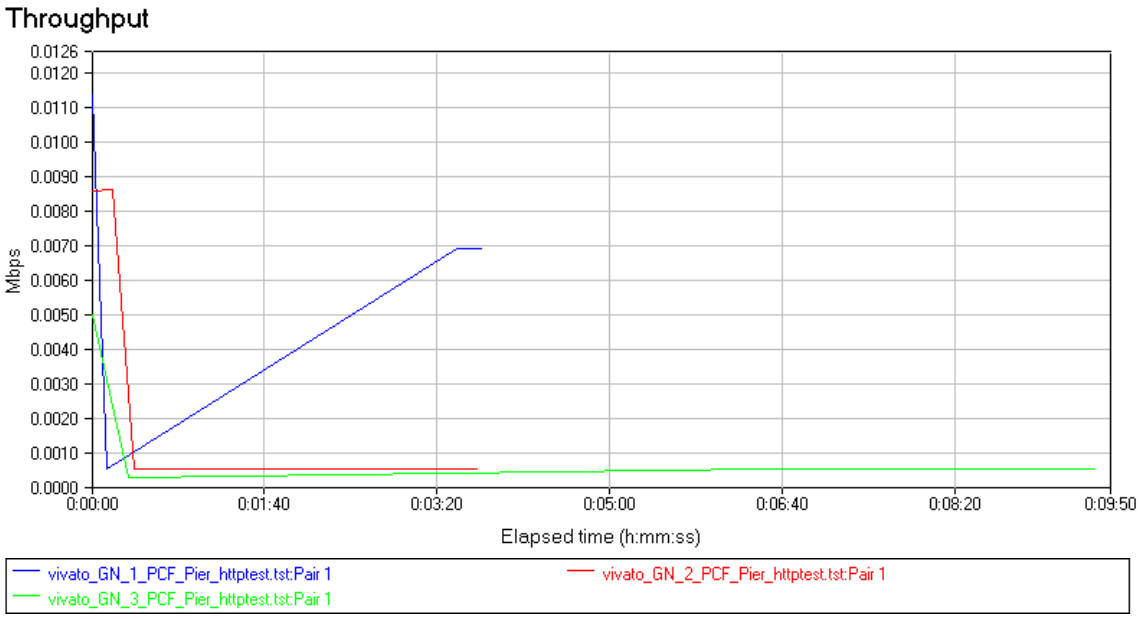

Figure 38. Pierside Throughput with GHOSTNet enabled.

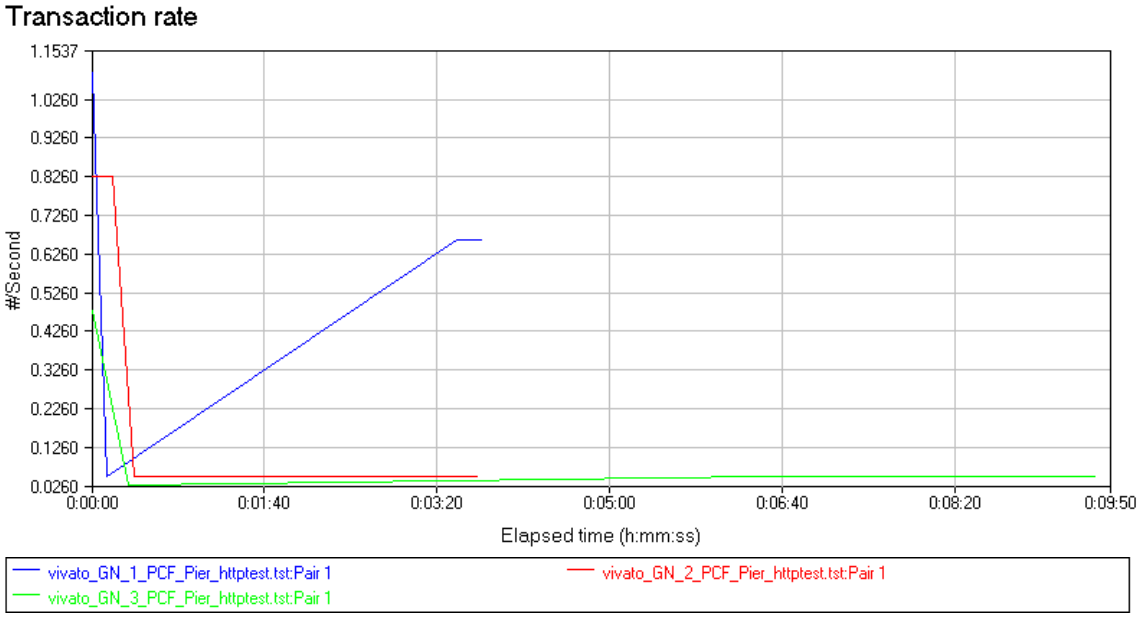

Figure 39. Pierside Transaction Rate with GHOSTNet enabled.

From Figures 37–39, the average Response Time measured with GHOSTNet enabled was 11.4763 seconds with a minimum time of 0.914 seconds and a maximum time of 38.854 seconds. The average Throughput measured was 0.001 Mbps with

a minimum of 0.000 Mbps and a maximum of 0.011 Mbps. The average Transaction Rate measured was 0.106 transactions per second with a minimum rate of 0.027 per second and a maximum rate of 1.094 per second.

In Figures 40–42, only two of the test runs (test runs two and six) could be used in the analysis. The other four test runs were very close to timing out and as a result were extremely inaccurate, producing asymptotic-like results. The average Response Time measured without GHOSTNet was 0.091 seconds with a minimum time of 0.015 seconds and a maximum time of 0.312 seconds. The average Throughput measured was 0.366 Mbps with a minimum of 0.033 Mbps and a maximum of 1.020 Mbps. The average Transaction Rate measured was 35.337 transactions per second with a minimum rate of 0.054 per second and a maximum rate of 64.935 per second.

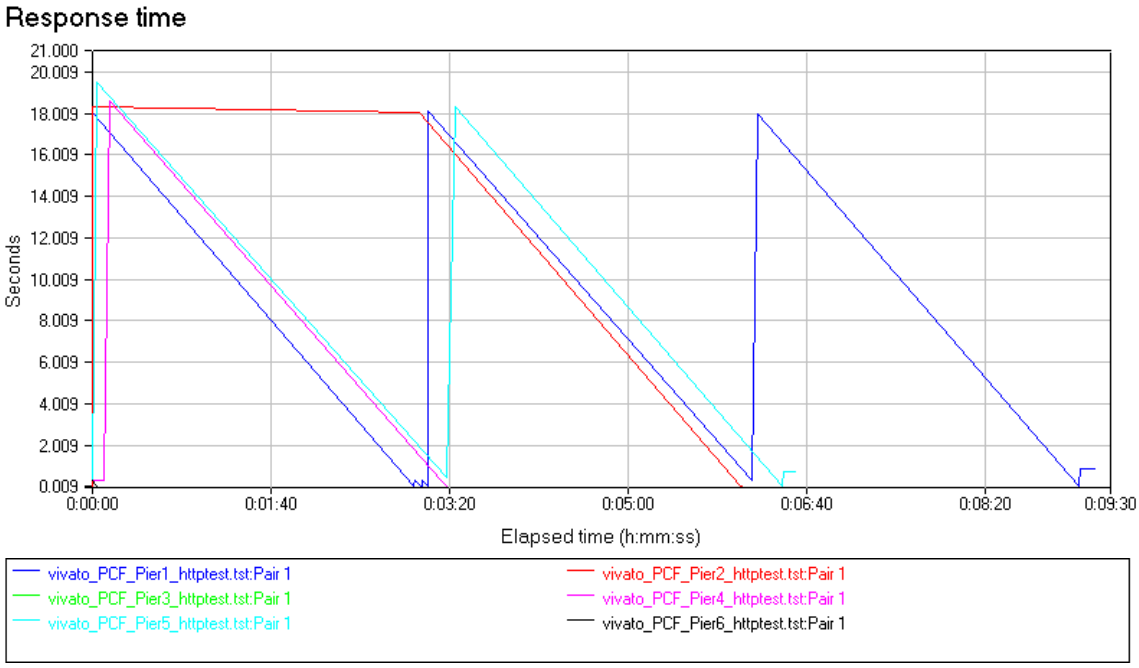

Figure 40. Pierside Response Time without GHOSTNet.

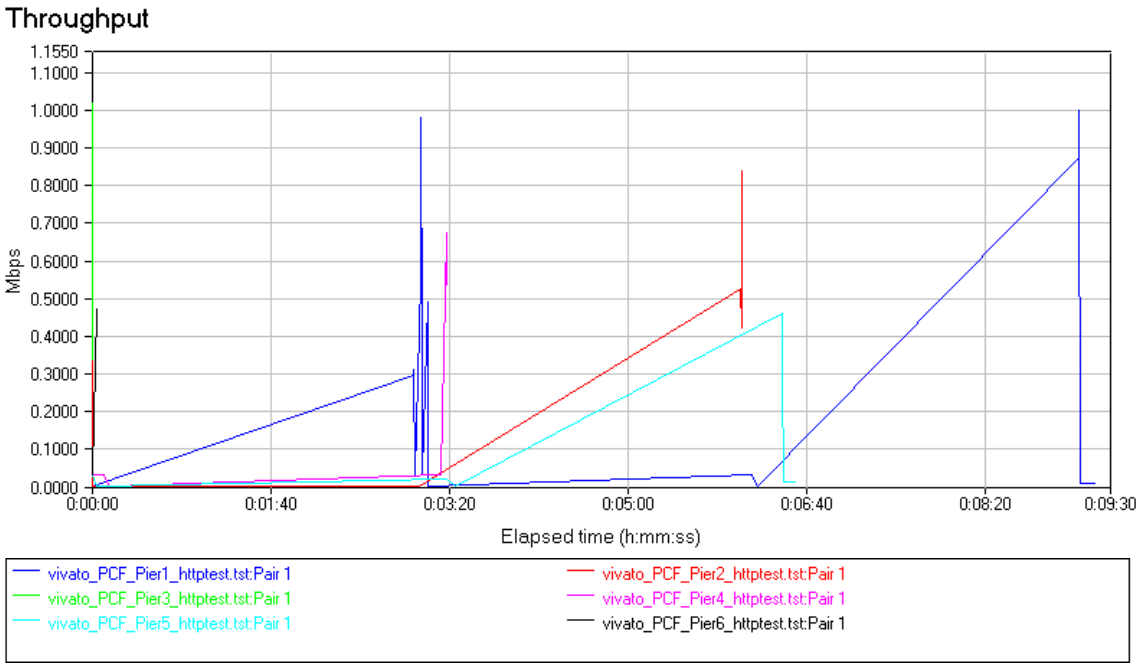

Figure 41. Pierside Throughput without GHOSTNet.

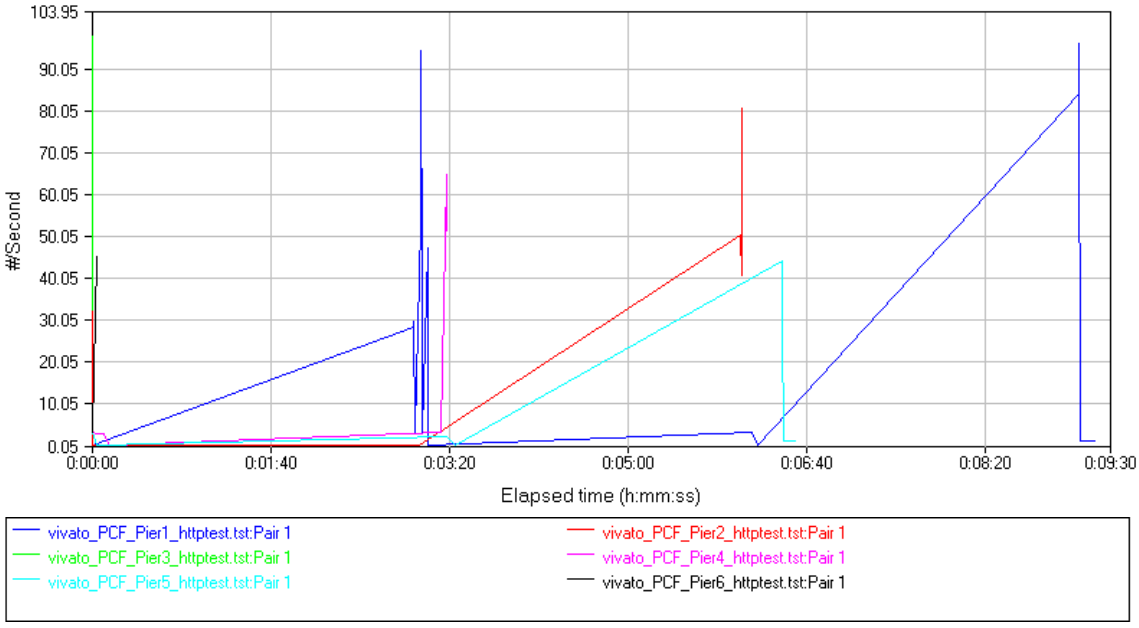

Figure 42. Pierside Transaction Rate without GHOSTNet.

3. Observations and Further Analysis from Thailand Field Testing

Overall, the field testing conducted in Thailand was successful. The results validated the hypothesis that phased array antenna technology could duplicate and exceed the performance on Monterey Bay during proof of concept testing. Performance limitations were noted in the conduct of testing which have to do with the mounting of the wireless router on the underway vessel. This and other issues will be discussed in greater depth below and in the Conclusions and Recommendations section, Chapter VII, respectively.

a. Exclusion of Outliers

The test runs that produced outliers in the data are excluded from the analysis of the specific group of test runs. The outliers are defined as results with 95% confidence intervals that did not overlap with the other recorded data sets in the group. This indicates that the outliers were more than two standard deviations away from the other data collected. The data represented in these outliers is inaccurate and would have negatively skewed the results of the analysis if included. Other characteristics of these outliers is the specific test runs (that produced them) took approximately 2-3 times longer to execute than the other test runs in the group. This is another symptom indicating an error in the conduct of the test run.

b. Power Issues

The unpredictable supply of power on the Ao Manao Airbase was an ongoing challenge throughout field testing in

Thailand. The base power distribution was subject to frequent power surges, or brief spikes in voltage, and brownouts, brief decreases in voltage. The performance of the testing hardware was affected by these fluctuations in the power. As a result, each of the phased array antenna base stations were directly connected to uninterruptable power supplies (UPS). The base stations run off DC power and utilize a power supply which converts 110VAC power to 48VDC and is directly wired to the panel. The panels' power supplies were plugged into UPS' (which were connected to step-down transformers which converted the 220V/50Hz power, from the base power grid, to 110V/60Hz power) for the power supplies to convert and supply steady, reliable power to the base stations. Two of the base station power supplies were rendered inoperable due to the power fluctuations experienced at Ao Manao Airbase. One of the power supplies was connected to an UPS, but it was not powered "ON," and was therefore unable to provide the necessary protection.

c. Speed vs. Latency

At first glance, the results of the network performance tests, especially in throughput, seem to be very low and not impressive. However, the more important question of performance is not raw throughput, but rather the amount of latency present. High throughput of 11 Mbps combined with high latency translates into poor network performance and is no better than the throughput results seen in the field tests with low latency. The ability of the network to pass the data packets was more than sufficient for the application. This is especially true, keeping in mind the

relationship between data rate and throughput as discussed in the Technical Background, Chapter II, A.3.—*Data Rate vs. Throughput*.

d. GHOSTNet Latency Resolved

Although resources were unavailable to properly resolve the latency issue attributed to tests involving GHOSTNet until February 2009, this issue has been corrected. The initial hypothesis was that the poor network performance noted in tests with GHOSTNet enabled was caused by the connections through servers in New Haven, Connecticut and Greensboro, North Carolina. To help prove this theory, an additional GHOSTNet server was established in Monterey, California and endpoint tests were run with GHOSTNet enabled. Significant improvements were seen in the test results, compared to those recorded at FEX IV, in the areas of Throughput, Response Time, and Transaction Rate. More in-depth analysis and conclusions were made in a separate thesis about GHOSTNet referenced here.[14]

[14] Patrick Kilcrease, "Employing a secure virtual private network (VPN) infrastructure as a global command and control gateway to dynamically connect and disconnect diverse forces on a task force by task force basis." Naval Postgraduate School, September 2009.

V. CONCLUSIONS AND RECOMMENDATIONS

A. OVERVIEW

Although less than 100% of the data was successfully collected in each of the test runs of the six groups of test operating environments, there are significant advances for backhaul communications related to ship-to-shore and ship-to-ship test engagements that are prime candidates for data collection. Future follow-on iterations of field tests with phased array antenna technology could build on these measures of effectiveness and utilize the conclusions and recommendations made below.

B. CONCLUSIONS AND KEY TAKEAWAYS

1. Environmental Impacts on Network Performance

The most significant environmental limitations encountered during testing were latency as a direct result of encryption, LOS obstruction, and power fluctuations. The GHOSTNet server latency issue was resolved, as noted above, but LOS continues to be a challenging obstacle to overcome in a dynamic operating environment. Pierside in the north bay, ships across the pier with taller superstructures impeded the conduct of network performance tests from the PCF. The vessels created significant interference as they physically obstructed the LOS of the base station and the antenna device mounted on the mast of the PCF.

During the 1NM underway test in the south bay, it was noted that dense foliage from trees and other vegetation were preventing the necessary LOS for the wireless signal to reach the PCF from the Comms Tower. The geometry of the situation in the south bay was more favorable once the PCF was near the 2NM point from the Comms Tower. This is why test results were more favorable at a greater distance vice being closer to the signal in the south bay.

As previously noted, power fluctuations on the base in Thailand posed the most significant challenges to the performance of the wireless network. The heat and humidity of the physical operating environment had much less impact than originally anticipated. In fact, successful end-to-end tests were conducted during the rainstorm encountered on the second day of testing.

2. Effective Range of Wireless Coverage

Due to time and weather constraints impacting the conduct of further underway field tests, the maximum effective range underway was unable to be determined. It should be noted, however, that the capability to view live video over a wireless network at distances up to and greater than 2NM (2.3 miles) is a significant achievement. An existing operational deployment of two base stations on the Outer Banks, North Carolina covers 15 square miles.[15] This documented operational deployment far exceeds the 2NM effective range tested in this research. Therefore, the wireless network provided by the phased array antennas

[15] Gardner, David, W. Town picks WiFi over WiMAX for public network. May 19, 2005. http://commsdesign.com/showArticle.jhtml?articleID=163105779.

deployed in Thailand, was reliable within the envelope of two “plus” nautical miles (2+NM) and beyond. Given the notional throughput expected from the modulation scheme utilized for the specific data rate at these distances, the results are in line with factory specifications and can be predictable variables given the operational environment.[16]

3. GHOSTNet Application

GHOSTNet was a viable tool for securing the communications over the wireless network environment established during field testing in Thailand. Its ability to quickly and easily connect disparate personnel and improve their SA on a situation taking place halfway around the world was noteworthy. GHOSTNet was a true value added component of this research and has many, far-reaching applications for further development and implementation.[17]

4. Ruckus Wireless Device

The Ruckus device certainly allowed for the maximum reception of the 802.11g signal, from the phased array antennas on the Comms Tower, inside the pilothouse of the PCF while underway and pierside by utilizing the bridge mode. The connectivity provided by the device and its ability to maintain association with the wireless base stations while underway was not reliable when the PCF was constantly changing aspect. The sectored antennas ability to dynamically associate when the PCF was facing away from the Comms Tower was suspect. The Ruckus device would lose

---

[16] Carpenter and Barrett, Certified Wireless Network.

[17] Kilcrease, *Employing a secure virtual private network (VPN) infrastructure*.

connectivity in a 30-degree cutout facing aft of the PCF, as shown in Figure 43. When the bearing to the Comms Tower was orientated aft of the PCF, within this 30-degree cut-out, the association of the Ruckus to the wireless network was lost. As the PCF's orientation changed, and the bearing to the Comms Tower was not within this sector, the device would re-associate with the network. Any data or video that was previously being transferred before the drop in connectivity was not received by the intended user. This process of re-association to the wireless network and then re-initiating the transfer of data took a few minutes to accomplish for each occurrence. This did present a challenge when transferring data, but proved to be a significant issue when transmitting streaming video, especially as the bearing to the Comms Tower was constantly changing due to the vessel being underway. The signal was interrupted and any video captured while the device was in the process of re-association with the wireless network was never seen by the intended remote stations. Suggestions of how to better solve this issue are listed below in the recommendations section.

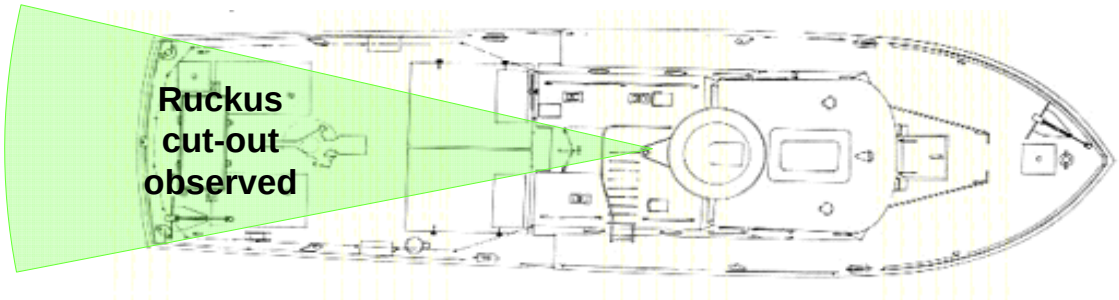

Figure 43. 30-degree cut-out aft experienced by Ruckus device mounted to mast of RTN PCF.

5. Wireless Network Scalability

Due to time constraints and power issues, insufficient testing with respect to multiple streaming video feeds was conducted to make a clear determination of how this would affect the scalability of the wireless network. The fluctuations in power rendered a fourth wireless base station inoperable. This additional wireless panel, separate from the three mounted on the Comms Tower, was overlooking the south bay from the Ao Manao Hotel/BOQ, seen in Figure 44 and theoretically would have improved the conduct of underway tests executed in the south bay by providing better coverage.

What is known is that if the challenge of wirelessly associating to the network while changing aspect in an underway vessel can be improved, the wireless network is capable of being applied to real-world environments. Recommended solutions to this problem are listed below and in the next section. The current configuration of technology could be deployed as-is to port security elements that carry out inspections on ships at anchor and/or pierside, where a less dynamic change in aspect would allow the smart router to remain associated to the wireless network. The phased array antenna technology is more than capable of scalability for real-world applications and its primary limitation is the performance and capabilities of the receiving antenna employed by the end user.

Figure 44. Wireless base station overlooking south bay, from the 4th floor roof access of the Ao Manao Hotel.

C. RECOMMENDATIONS FOR FUTURE STUDY AND APPLICATION

1. Utilizing an Omnidirectional Antenna Underway

Employing an omnidirectional antenna with the technological configuration outlined in the field testing would potentially resolve the association/disassociation issues experienced by the dynamically adjusting antennas in the Ruckus device and could increase performance of the wireless network. The dipole antenna construction of the omnidirectional antenna is much better suited to this application, as its receiving gain pattern is 360 degrees on a horizontal plane. Furthermore, the omnidirectional antenna should be utilized when the location of the receiver is "highly mobile."[18]

[18] Dean, Network+ Guide to Networks, 125.

The Ruckus device, and its six, dynamically adjusting sectored antennas, was acting primarily as a wireless bridge by linking the wireless network of the phased array antennas and the PCF. Bridge mode is not the optimal performance configuration in this specific application, as the bearing to the wireless signal was constantly changing. The Ruckus would be much better suited to operate in route mode to extend the wireless footprint and quality of the 802.11g signal, received by the omnidirectional antenna, from the phased array base stations to the immediate vicinity of the PCF where it would be mounted. Although this configuration was unable to be field tested, it is recommended as the optimal solution to the specific application based on the testing and observations noted in this research.

2. Integrated Video/Voice Application Underway

An IP-routable camera with a microphone or an audio line into the feed should be explored to enable simple, two-way video and voice communication. This could be implemented in a variety of COTS hardware or software solutions. Skype, an internet video/voice application, was successfully utilized via the wireless network to communicate between the JOCC and the PCF during the storm, on the second day of testing. While the PCF was pierside in the north bay, and the ships obstructing the wireless signal had gone out to sea, RTN personnel were able to quickly and easily interact using this internet application.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A – WEATHER DATA

#YY	MM	DD	hh	Mm	WVHT	WVHT
#yr	mo	dy	hr	Mn	m	ft
2008	2	14	9	23	3.35	10.99
2008	2	14	9	53	3.12	10.24
2008	2	14	10	23	3.14	10.30
2008	2	14	10	53	2.83	9.28
2008	2	14	11	23	3.28	10.76
2008	2	14	11	53	3.12	10.24
2008	2	14	12	23	2.96	9.71
2008	2	14	12	53	3.03	9.94
2008	2	14	13	53	3.16	10.37
2008	2	14	14	23	3.05	10.00
2008	2	14	14	53	2.88	9.45

Table 6. Wave height data (in meters and feet) for Monterey Bay, CA on February 14, 2008 (from NOAA Web site).

Time (PST):	Temp.:	Dew Point:	Humidity:	Sea Level Pressure:	Visibility:	Wind Dir:	Wind Speed:	Gust Speed:	Precip:	Conditions:
8:54 AM	55.0 °F	21.0 °F	27%	30.04 in	10.0 miles	NW	6.9 mph	-	N/A	Clear
9:54 AM	55.9 °F	21.0 °F	26%	30.06 in	10.0 miles	Variable	4.6 mph	-	N/A	Clear
10:54 AM	60.1 °F	16.0 °F	18%	30.05 in	10.0 miles	NNE	15.0 mph	26.5 mph	N/A	Clear
11:54 AM	62.1 °F	12.9 °F	15%	30.05 in	10.0 miles	NNE	15.0 mph	23.0 mph	N/A	Clear
12:54 PM	61.0 °F	21.9 °F	22%	30.04 in	10.0 miles	NW	10.4 mph	16.1 mph	N/A	Clear
1:54 PM	61.0 °F	30.0 °F	31%	30.03 in	10.0 miles	NW	9.2 mph	-	N/A	Clear
2:54 PM	62.1 °F	26.1 °F	25%	30.04 in	10.0 miles	WNW	9.2 mph	-	N/A	Clear

Table 7. Weather data points for Monterey Bay, CA on February 14, 2008 (from Weather Underground Web site).

Time (ICT):	Temp.:	Dew Point:	Humidity:	Sea Level Pressure:	Visibility:	Wind Dir:	Wind Speed:	Gust Speed:	Precip:	Events:	Conditions:
8:00 AM	80°F	75.5°F	76%	29.79 in	4 miles	ESE	1 mph	-	-		Mostly Cloudy
9:00 AM	83°F	76°F	76%	29.89 in	5 miles	ESE	2 mph	-	-		Mostly Cloudy
10:00 AM	87°F	77°F	75%	29.89 in	6 miles	ESE	3 mph	-	-		Clear
11:00 AM	89°F	78°F	74%	29.89 in	6 miles	ESE	4 mph	-	-		Clear
12:00 PM	92°F	79°F	74%	29.86 in	6 miles	ESE	5 mph	-	-		Clear
1:00 PM	95°F	80°F	74%	29.86 in	6 miles	ESE	6 mph	-	-		Clear
2:00 PM	93°F	79°F	74%	29.80 in	6 miles	ESE	5 mph	-	-		Clear
3:00 PM	92°F	78°F	74%	29.77 in	5 miles	ESE	4 mph	-	-		Mostly Cloudy

Table 8. Weather data points for Prachuap Khiri Khan, Thailand, on March 24, 2008 (from Weather Underground Web site).

Time (ICT):	Temp.:	Dew Point:	Humidity:	Sea Level Pressure:	Visibility:	Wind Dir:	Wind Speed:	Gust Speed:	Precip:	Events:	Conditions:
8:00 AM	79°F	75°F	75%	29.79 in	4 miles	Calm	Calm	-	N/A		Mist
9:00 AM	77.5°F	77°F	75%	29.89 in	5 miles	Calm	6.9 mph	-	N/A		Mostly Cloudy
10:00 AM	77°F	77°F	75%	29.89 in	2 miles	ESE	7 mph	-	-	Rain	Light Rain
11:00 AM	76°F	75.2°F	74%	29.89 in	2 miles	ESE	11.5 mph	25mph	-	Thunderstorm	Heavy Rain
12:00 PM	76.5°F	75.2°F	74%	29.86 in	3 miles	SE	5 mph	-	-	Rain	Light Rain
1:00 PM	76°F	74 °F	74%	29.86 in	5 miles	South	5 mph	-	N/A		Mostly Cloudy
2:00 PM	76.5°F	77°F	74%	29.80 in	5.6 miles	South	6 mph	-	N/A		Mostly Cloudy
3:00 PM	77°F	77°F	74%	29.77 in	5.6 miles	South	5 mph	-	N/A		Mostly Cloudy

Table 9. Weather data points for Prachuap Khiri Khan, Thailand, on March 25, 2008 (from Weather Underground Web site).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B – TECHNICAL SPECIFICATIONS

VP2210 – Vivato 802.11g Outdoor Wi-Fi Base Station	
WIRELESS SPECIFICATIONS Network Standard	IEEE 802.11b/g
Frequency Band/Operating Channels	2.4 – 2.483 GHz, North America Channel Set (1–11)
Supported Data Rates	802.11b: 1,2,5.5,11Mbps 802.11g: 6,9,12,18,24,36,& 54Mbps
Media Access Protocol	Carrier Sense Multiple Access/ Collision Avoidance
Receive Sensitivity CCK: 8% PER, 1000 bytes OFDM: 10% PER, 1024 bytes	Rate (mode) receiver sensitivity 54 (OFDM) -72dBm 11 (CCK) -90dBm 48 (OFDM) -76dBm 5.5 (CCK) -93dBm 36 (OFDM) -81dBm 2 (CCK) -94dBm 24 (OFDM) -84dBm 1 (CCK) -95dBm 18 (OFDM) -87dBm 12 (OFDM) -90dBm 9 (OFDM) -91dBm 6 (OFDM) -92dBm
Operating Range	Outdoor Line of Sight: *Data Rate* *Range (meters)* *Data Rate* *Range (meters)* 54Mbps 650m 11Mbps 4,600m 48Mbps 900m 5.5Mbps 5,250m 36Mbps 1,400m 2Mbps 5,400m 24Mbps 1,800m 1Mbps 5,500m 18Mbps 2,300m 12Mbps 2,950m 9Mbps 3,200m 6Mbps 3,500m
Users per Device	Up to 50 simultaneous users/1,530 associated users
EIRP (Max.)	41dBm typical @ 802.11b rates, 21dBi antenna 37dBm typical @ 802.11g rates, 21dBi antenna
WIRED SPECIFICATIONS Network Interfaces	2 – IEEE 802.3 auto-sensing 10/100 Base T Ports
SECURITY Static and Dynamic WEP Encryption	40- and 104-bit (RC^4) Encryption
WPA	802.1x – EAP-TLS, EAP-TTLS, PEAP, TKIP/MIC
802.11i/WPA2	AES supported; 802.1x – EAP-TLS, EAP-TTLS, PEAP, TKIP/MIC
ICCF	Inter-client communication filtering
Multiple SSID/VLAN	Support for up to 16 MSSID/VLANs each capable of supporting a different security model
ENVIRONMENTAL SPECIFICATIONS Dimensions	30"(L) x 30"(H) x 11"(W)

VP2210 – Vivato 802.11g Outdoor Wi-Fi Base Station	
Power Requirement	48VDC, 200 Watts maximum
Weight	83lbs. (37.64Kg.)
Operating Temperature	-40°F to 131°F
CERTIFICATIONS Radio	 FCC 47 CFR Part 15, Class B Industry Canada RSS 210

Figure 45. Vivato technical specifications (from Vivato Web site).

Ruckus MediaFlex 2835 Smart Wi-Fi Router	
Physical Characteristics Power	 External power adapter Input: 110-240V AC Input: 20-240V AC Output: 12V DC, 1A
Physical Size	14.2cm (L), 12.2cm (W), 7.5cm (H)
Weight	200 grams
Antenna	Internal software-configurable antenna array with six directional high-gain elements that provide up to 63 unique antenna patterns
Ethernet Ports	5 ports, auto MDX, autosensing 10/100 mbps, RJ-45
LED display	Power/status, Ethernet status, wireless status, wireless network quality indicator
Environmental conditions	Operating Temperature: 32°F (0°C)-104°F (40°C) Operating humidity: 15%-95% non-condensing
Performance and Supported Configurations Concurrent stations	 - Up to 48 (open, WEP or WPA-AES) - Up to 22 (for WPA-TKIP)
Target UDP throughput	15-20 Mbps (54 Mbps bursts) sustainable throughout a 4000 square foot (372m^2) public area
Simultaneous video transmission	2 to 3 simultaneous MPEG-2 or 4 to 6 MPEG-4 standard definition streams or single 10Mbps+HD stream with concurrent background traffic
Traffic Management and Quality of Service Classes of service	 Voice, video, best effort and background
Authentication/Tunneling	- L2TP (secure and unsecure) - IPSEC
MAC address entries	128
Access control	Layer 2 MAC addresses Layer 3 IP addresses Layer 4 TCP ports
Management (when individually managed)	

Ruckus MediaFlex 2835 Smart Wi-Fi Router	
Configuration	Web user interface, TR-069, Bonjour, CLI (Telnet), SSH HTTP/S, SNMP statistics interface
Login	User Administrator
Statistics	LAN, wireless and associated stations (accessible via Web UI)
Software update	- FTP or TFTP, remote auto available - Accessible via WebUI
Wi-Fi Standards	 802.11b/g
Supported data rates	54,48,36,24,18,12,11,5.5,2,1Mbps
Channels	US/Canada: 1-11 Europe (ETSI X30): 1-13
Auto channel selection	Supported
RF power output	23 dBm for wireless-B 23 dBm for wireless-G - Country-specific power settings are configurable
Transmit power control	Supported
BSSID	Up to four
Power Save	Supported
Certifications	FCC (U.S.), CE (EU), OFTA (Hong Kong), IC (Canada), C-Tick (Aus/ NZ), IDA (Singapore), MIC (Korea), DGT (Taiwan) WEEE/ROHS compliance
Wireless Security	WEP, WPA-PSK, WPA-TKIP, WPA2-AES
Routing	DHCP client support, DHCP server support, NAT and PPPoE
Multicast Video Multicast operations	 -Directs multicast IPTV packets to each receiving station within the designated multicast group using the optimum data rate and antenna selection -Automatic classification into video

Figure 46. Ruckus technical specifications (from Ruckus Web site).

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Chief of Naval Operations. "CNO Guidance for 2007-2008: Executing our Maritime Strategy." CNO, October 25, 2007.

———. "Cooperative Strategy for 21St Century Seapower." CNO, October 17, 2007.

———. "Navy Maritime Domain Awareness Concept." CNO, May 29, 2007.

Carpenter, Tom, and Joel Barrett. Certified Wireless Network Administrator Official Study Guide, Fourth Edition. August 17, 2008, 116.

Cisco White Paper. "Capacity Coverage & Deployment Considerations for IEEE 802.11g." Cisco Systems, Inc. 2005. http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_white_paper09186a00801d61a3.shtml, accessed March 25, 2008.

Clark, Vern, ADM. *Sea Power 21: Projecting Decisive Joint Capabilities.* Proceedings, US Navy Institute Press, October 2002. http://www.navy.mil/navydata/cno/proceedings.html, accessed March 23, 2008.

Cross, Eric C. "Modern Advances to the Modular Fly-Away Kit (MFLAK) to Support Maritime Interdiction Operations." Naval Postgraduate School, September 2007.

Dean, Tamera. Network+ Guide to Networks, Fourth Edition. April 4, 2005, 388-402.

Feilner, Markus. OpenVPN: Building and Integrating Virtual Private Networks: Learn how to build secure VPNs using this powerful Open Source application. November 5, 2006, 10-21.

Filtikakis, Stefanos. "Performance Analysis of IEEE 802.11g Signals Under Different Operational Environments." Naval Postgraduate School, September 2005.

Gardner, David, W. *Town picks WiFi over WiMAX for public network.* May 19, 2005. http://commsdesign.com/showArticle.jhtml?articleID=163105779, accessed April 8, 2009.

Gast, Matthew. 802.11 Wireless Networks: The Definitive Guide, Second Edition. April 25, 2005, 276–310.

Kilcrease, Patrick. “Employing a secure virtual private network (VPN) infrastructure as a global command and control gateway to dynamically connect and disconnect diverse forces on a task force by task force basis.” Naval Postgraduate School, September 2009.

Klopson, Jadon E. and Stephen V. Burdian. "Collaborative Applications used in a Wireless Environment at Sea for use in Coast Guard Law Enforcement and Homeland Security Missions." Naval Postgraduate School, March 2005.

Lounsbury, Robert Lee Jr. "Optimum Antenna Configuration for Maximizing Access Point Range of an IEEE 802.11 Wireless Mesh Network in Support of Multimission Operations Relative to Hastily Formed Scalable Deployments." Naval Postgraduate School, September 2007.

Proxim White Paper. "A Detailed Examination of the Environmental and Protocol Parameters that Affect 802.11g Network Performance." Proxim Corporation, 2003. http://www.proxim.com/learn/library/whitepapers/parameters_802.11g_performance.pdf, accessed March 23, 2008.

Vivato Case Study. “Newport, Rhode Island: A Large Metropolitan ‘Hot Zone’ Provides Broadband Ship-to-Shore Communications.” Vivato, Inc., 2003.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Mr. James F. Ehlert
   Naval Postgraduate School
   Monterey, California

4. Mr. Buddy Barreto
   Naval Postgraduate School
   Monterey, California

5. Mr. John Spracklen
   Southwest Data Centers
   Las Vegas, Nevada

6. Mr. Ryan Hale
   Kestrel Technology Group LLC
   Sugarland, Texas

7. Mr. Ed Fisher
   Naval Postgraduate School
   Monterey, California